

Особенности настройки встроенного фаервола Windows

windowsnotes.ru/other/osobennosti-nastroyki-vstroennogo-faervola-windows

1 августа 2024 г.

Что можно сказать о встроенном фаерволе Windows? Если коротко — он есть, и, в принципе, задачи свои выполняет. Но есть нюансы 😊

Встроенный межсетевой экран (он же фаервол, он же брандмауэр) появился еще в Windows XP под названием Internet Connection Firewall (ICF). Функционал у него был довольно бедный, настройки производились вручную под каждый сетевой интерфейс, кроме того он не умел фильтровать исходящий трафик. Из-за проблем с совместимостью он по умолчанию был выключен, а из-за того, что его настройки находились в конфигурации сети, многие пользователи не находили их и не могли его включить.

С выходом Windows XP SP2 ситуация изменилась. Была значительно улучшена функциональность фаервола, полностью переработан интерфейс управления, а сам фаервол был переименован в Windows Firewall. По умолчанию он был включен и через него фильтровались все сетевые подключения. Появилась возможность логирования подключений, управление правилами через групповые политики, сетевые профили и многое другое. Но фильтрация исходящего трафика в нем по-прежнему отсутствовала.

В Windows Vista\Server 2008 фаервол наконец-то обрел возможность фильтровать исходящий трафик. Количество профилей увеличилось до трех — доменная, частная и публичная сеть. Появилась возможность использовать расширенный фильтр пакетов и применять правила к определенным диапазонам IP-адресов и портов.

В таком примерно виде он и дошел до наших дней, и сейчас входит в состав операционных систем Windows под именем Windows Defender Firewall (фаервол защитника Windows).

На этом заканчиваем с историей и переходим к более практичным вещам.

Профили

Каждому сетевому подключению в Windows назначается один из трех сетевых профилей:

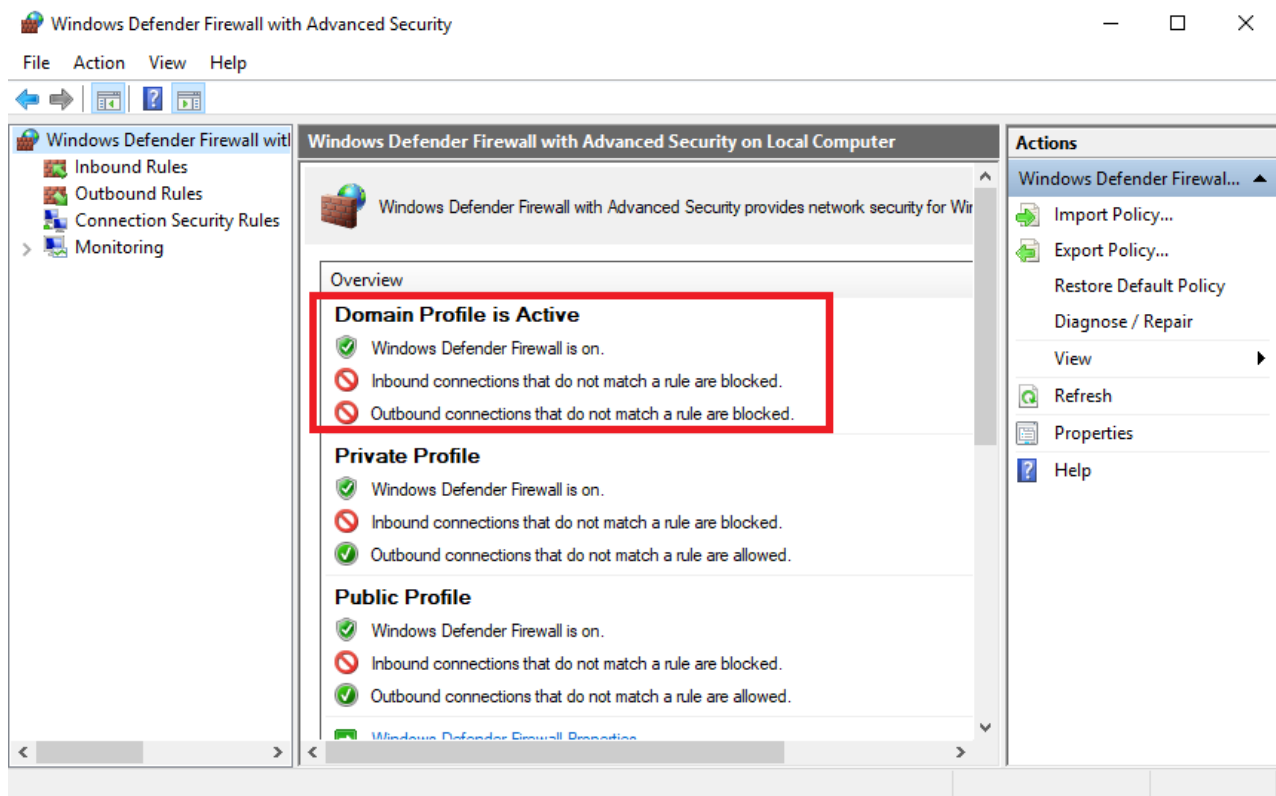
- **Private** — частная сеть. Это доверенная сеть, например домашняя или рабочая сеть в офисе. В частной сети компьютер будет доступен для обнаружения другими устройствами, на нем можно использовать службы общего доступа к сетевым файлам и принтерам;
- **Public** — общедоступная (общественная) сеть. Это недоверенная (небезопасная)

сеть, например Wi-Fi в кафе, в метро, аэропорту и т.п.. В такой сети не работает сетевое обнаружение, а также службы общего доступа к сетевым файлам и принтерам;

- **Domain** — доменная сеть. Сетевой профиль для компьютеров, которые находятся в корпоративной сети и присоединены к домену Active Directory.

Профиль определяется при подключении к сети. Если компьютер доменный и находится в доменной сети, то автоматически выбирается доменный профиль. В остальных случаях выбор делает пользователь, при подключении к сети. Впрочем, выбор этот в дальнейшем можно поменять.

В зависимости от профиля к сетевому интерфейсу могут применяться разные правила фаервола. Узнать, какой именно профиль активен в данный момент, можно из оснастки управления фаерволом. Открыть ее быстрее всего, нажав **Win+R** и выполнив команду **wf.msc**.

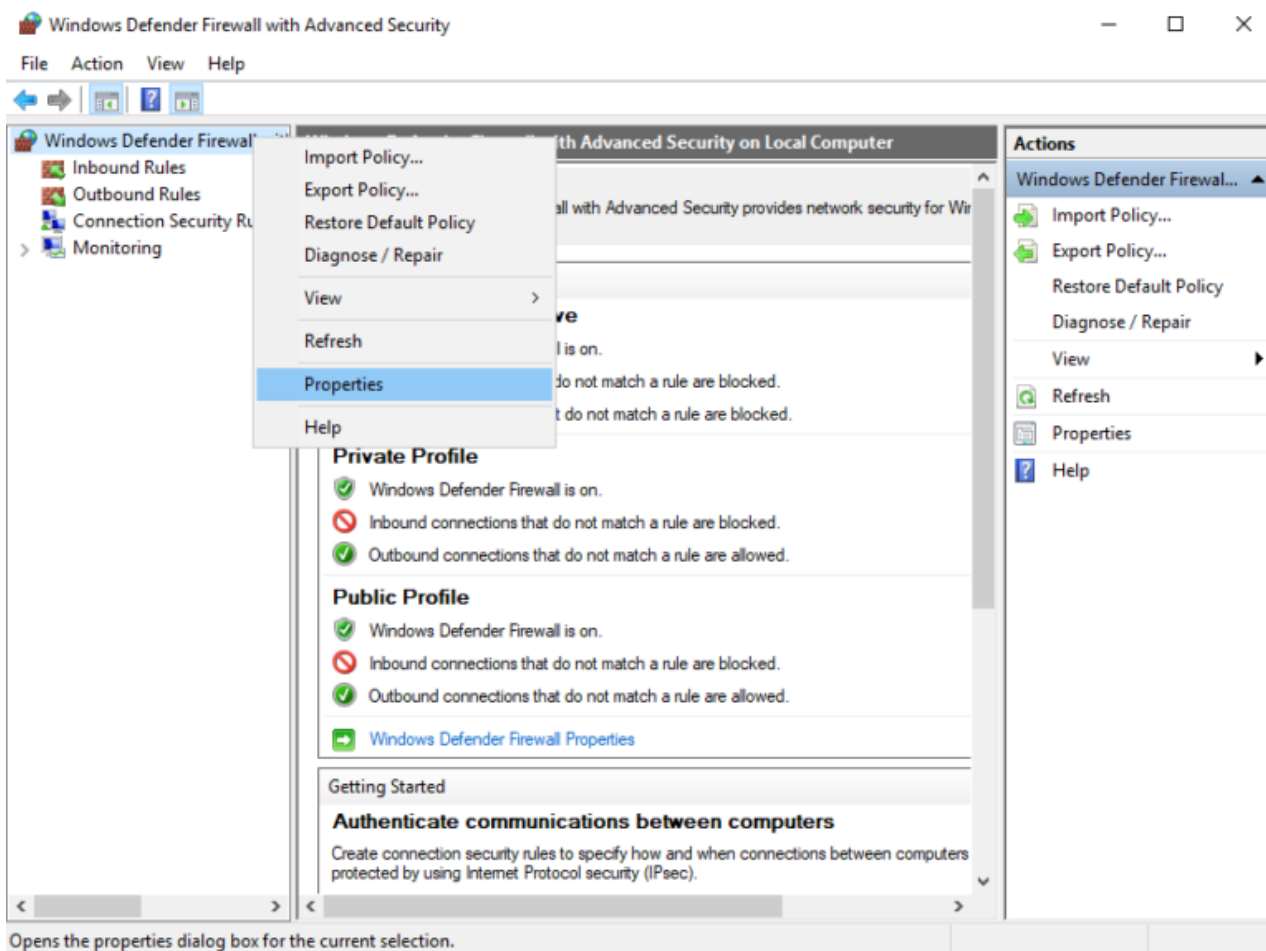


Режимы работы

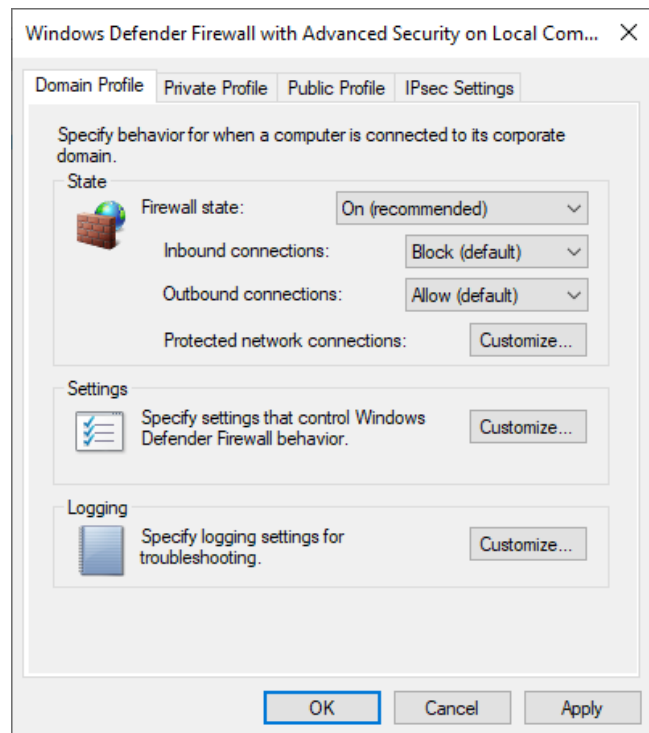
Для ограничения доступа обычно используются 2 различных подхода:

- Черный список — разрешено все что не запрещено;
- Белый список — запрещено все, что не разрешено.

В Windows Firewall по умолчанию используются оба подхода, причем одновременно. Чтобы убедиться в этом, откроем контекстное меню и перейдем к свойствам.



В открывшемся окне глобальные настройки фаервола, разбитые по профилям. Для каждого профиля мы можем включить\выключить фаервол, а также указать действие, которое будет применено к подключению, не подходящему под какое либо правило. Действия разделены, отдельно для входящего трафика, отдельно для исходящего. И для входящего трафика по умолчанию все, что не описано правилами, будет блокироваться (черный список), а для исходящего наоборот, все что не описано правилами будет пропускаться (черный список). Ну а поскольку каких либо запрещающих правил для исходящего трафика нет, то по умолчанию весь исходящий трафик никак не контролируется.



Типы правил

В документации [Microsoft](#) описаны следующие типы правил, которые поддерживает Windows Firewall:

- **Windows Service Hardening** — усиление защиты служб Windows. Тип встроенного правила, запрещающий системным службам устанавливать соединения способами, отличными от предусмотренных. Ограничения служб настраиваются таким образом, чтобы они могли взаимодействовать только указанными способами. Например, разрешенный трафик может быть ограничен указанным портом;
- **Connection security rules** — правила безопасности подключения. Этот тип правил определяет, правила аутентификации между двумя одноранговыми компьютерами, которые необходимо соблюсти, прежде чем они смогут установить соединение и обмениваться данными. Фаервол Windows использует протокол IPsec для обеспечения безопасности подключения за счет обмена ключами, проверки подлинности, обеспечения целостности данных и, при необходимости, шифрования данных;
- **Authenticated bypass rules** — аутентифицированные правила обхода. Этот тип правил разрешает подключение определенных компьютеров или пользователей, даже если входящие правила брандмауэра блокируют трафик. Это правило требует, чтобы сетевой трафик от авторизованных компьютеров аутентифицировался IPsec, чтобы можно было подтвердить личность. Например, вы можете разрешить удаленное администрирование брандмауэра только с определенных компьютеров, создав для этих компьютеров правила обхода с проверкой подлинности, или включить поддержку удаленной помощи со стороны службы поддержки. Правила такого типа иногда используются в корпоративных средах, чтобы разрешить «доверенным» анализаторам сетевого трафика доступ к компьютерам для помощи в устранении проблем с подключением. В правилах обхода перечислены

компьютеры, которым разрешено обходить правила, которые в противном случае блокировали бы сетевой трафик. Поскольку компьютер, на котором выполняется сетевой анализ, проходит аутентификацию и внесен в список «разрешенных» в правиле обхода, аутентифицированный трафик с этого компьютера разрешается через брандмауэр;

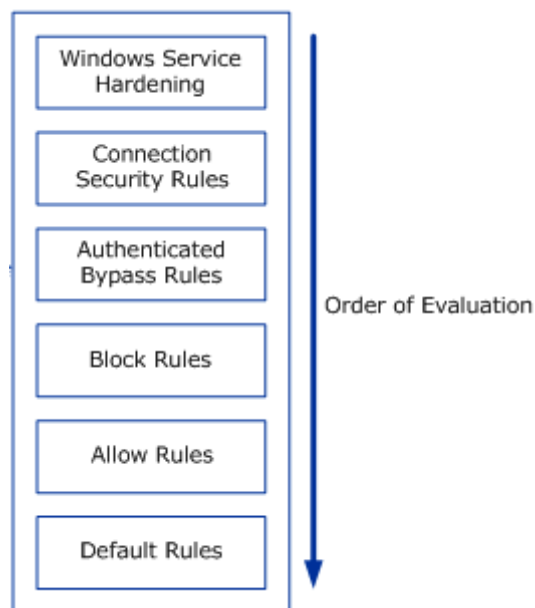
- **Block rules** — запрещающие правила. Этот тип правила явно блокирует определенный тип входящего или исходящего трафика;
- **Allow rules** — разрешающее правило. Этот тип правила явно разрешает определенный тип входящего или исходящего трафика;
- **Default rules** — правила по умолчанию. Эти правила определяют действие, которое происходит, когда соединение не соответствует никакому другому правилу.

Приоритет и порядок обработки правил

Вот порядок, в котором фаервол Windows обрабатывает различные типы правил. Такой порядок правил всегда соблюдается, независимо от происхождения правила (локальное или из групповой политики). Все правила, в том числе из групповой политики, сначала сортируются и уже затем применяются.

Исходя из порядка обработки, запрещающее правило имеет приоритет перед разрешающим, поскольку они обрабатываются раньше. Сетевой трафик, соответствующий как активному правилу блокировки, так и активному разрешению, блокируется.

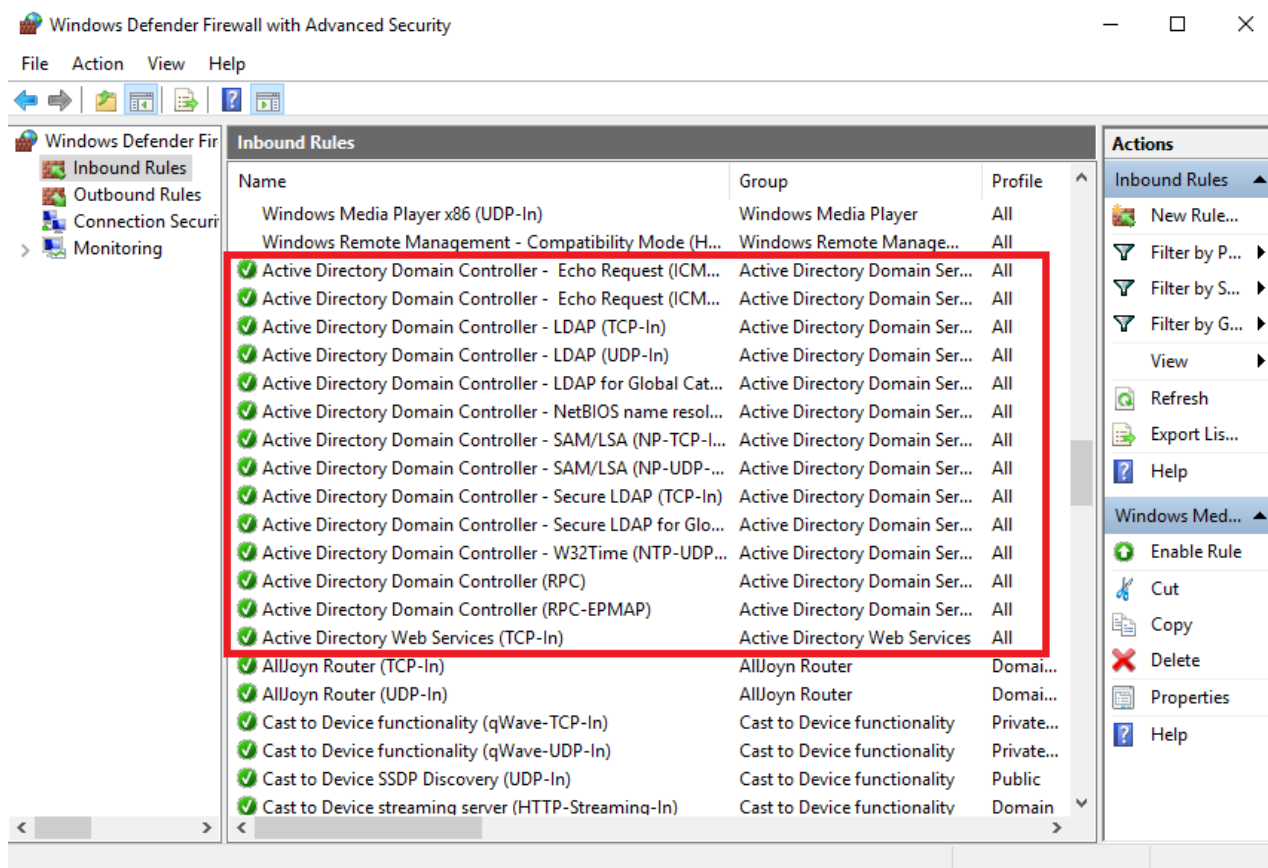
Что касается обработки правил одного типа, например разрешающих, то там какого либо порядка обработки и приоритета нет. Ищется любое подходящее правило, если его нет, то применяется правило по умолчанию.



Предопределенные правила

Если зайти в раздел с входящими или исходящими правилами, то мы увидим большое количество уже готовых, предопределенных (predefined) правил. Эти правила предназначены для обеспечения корректной работы операционной системы и ее компонентов. Некоторые правила включены по умолчанию, другие активируются по мере необходимости, например при установке серверной роли.

Для примера возьмем контроллер домена и посмотрим его входящие правила. Как видите, на нем активен набор правил, необходимых для работы Active Directory. Эти правила были активированы автоматически, при установке роли Active Directory Domain Services.




Особенностью встроенных правил является то, что их нельзя отредактировать. Можно включить или отключить правило, изменить действие (например с разрешения на запрет) но изменить сами настройки фильтра (протокол, порт и т.п.) невозможно.

Active Directory Domain Controller - LDAP (TCP-In) Properties

Protocols and Ports Scope Advanced Local Principals Remote Users

General Programs and Services Remote Computers

 This is a predefined rule and some of its properties cannot be modified.


General

Name: Active Directory Domain Controller - LDAP (TCP-In)

Description: Inbound rule for the Active Directory Domain Controller service to allow remote LDAP traffic. [TCP 389]

☒ Enabled

Action

 ☒ Allow the connection

☐ Allow the connection if it is secure

Customize...

☐ Block the connection


OK Cancel Apply

Active Directory Domain Controller - LDAP (TCP-In) Properties

General Programs and Services Remote Computers

Protocols and Ports Scope Advanced Local Principals Remote Users

Protocols and ports

 Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

389

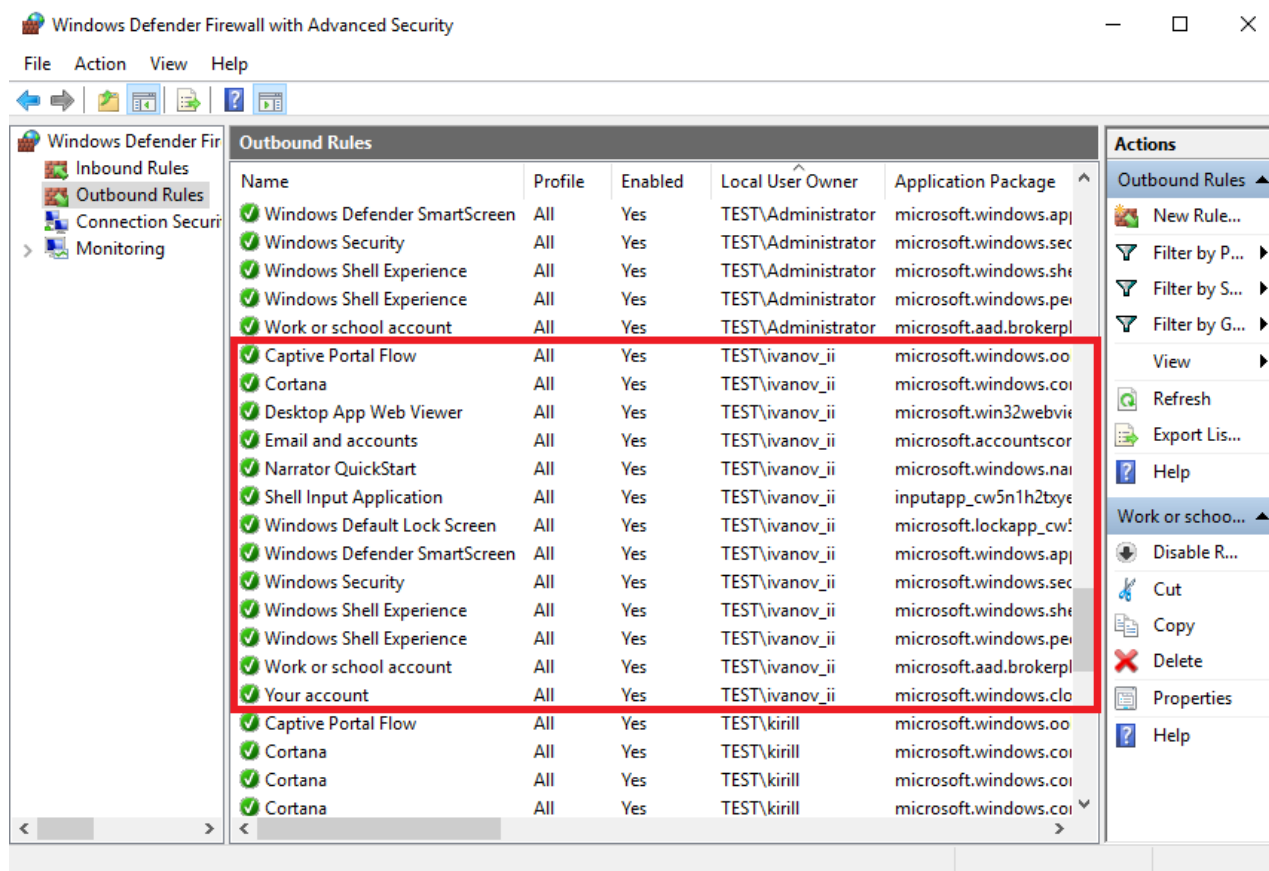
Remote port: All Ports

Internet Control Message Protocol (ICMP) settings: Customize...

OK Cancel Apply

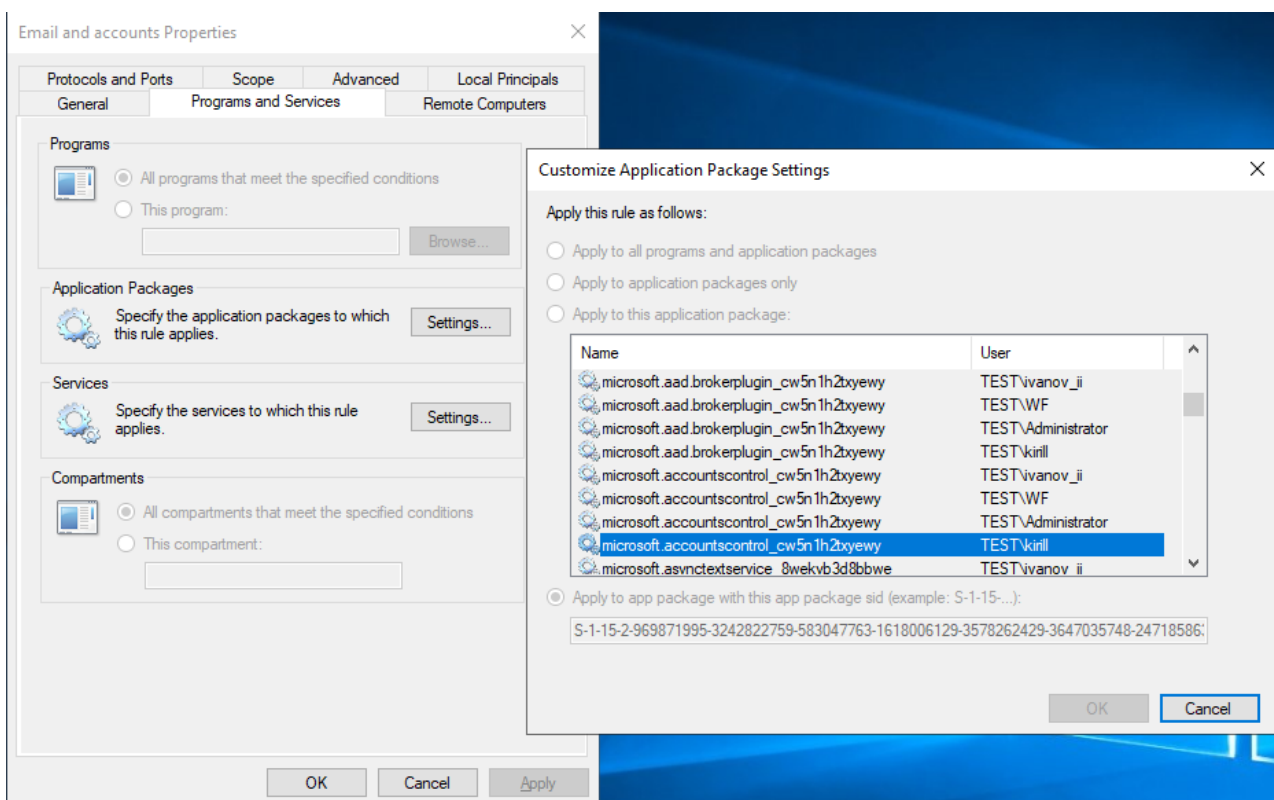
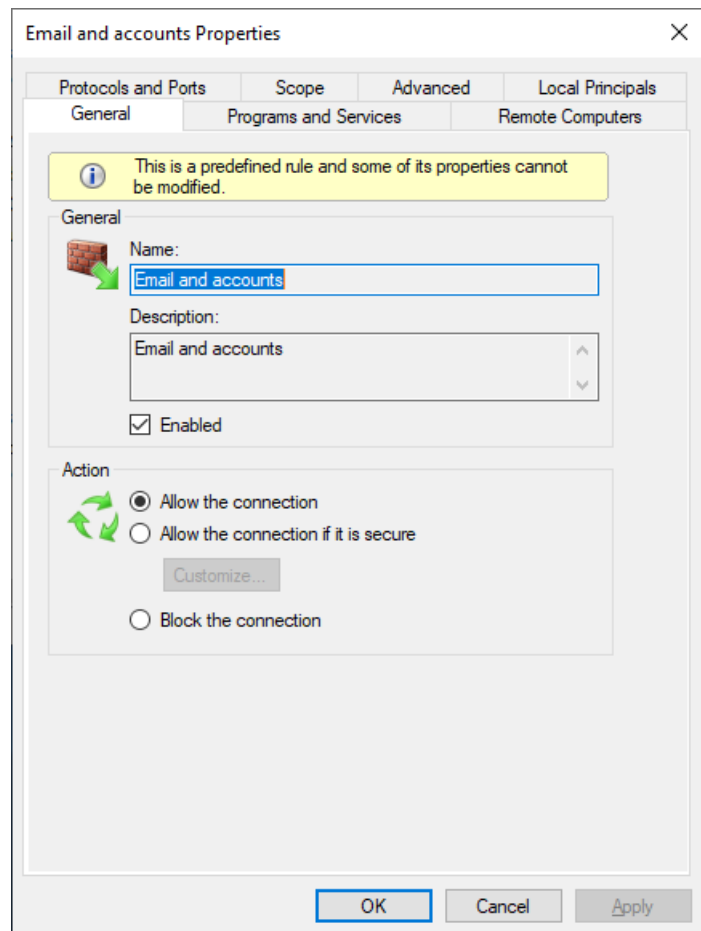
Автоматически сгенерированные правила

Еще один тип правил — это правила, автоматически генерируемые системой. Они создаются для каждого пользователя при входе в систему. Их отличительной особенностью является наличие владельца в поле Local User Owner.



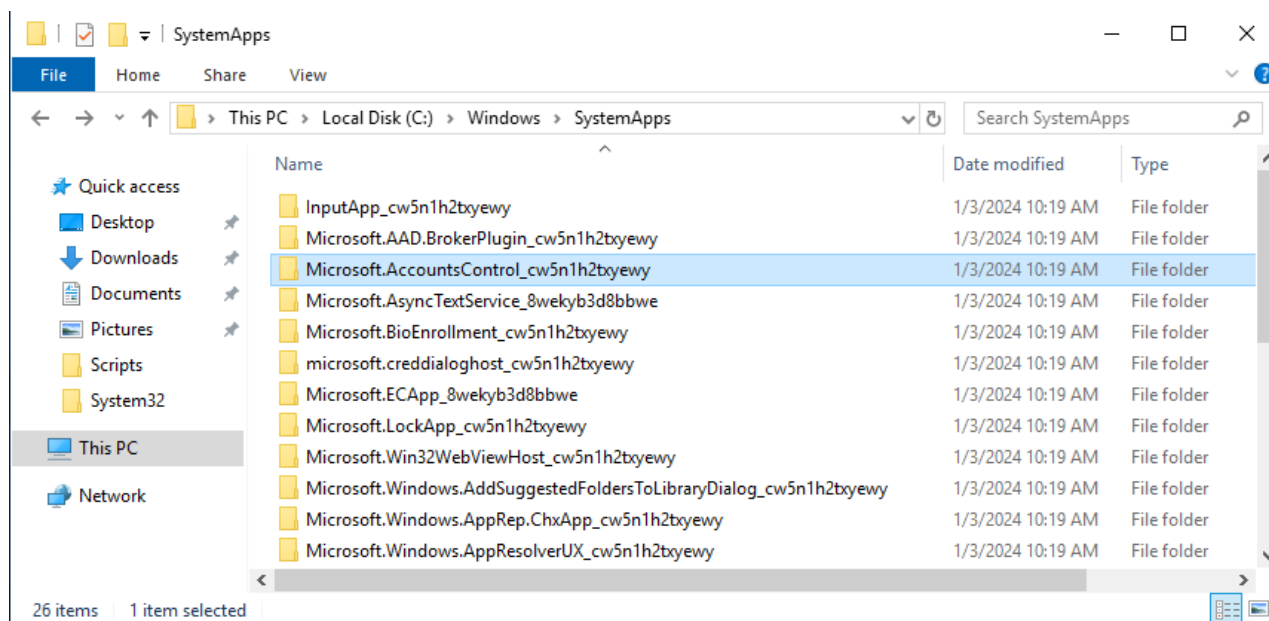
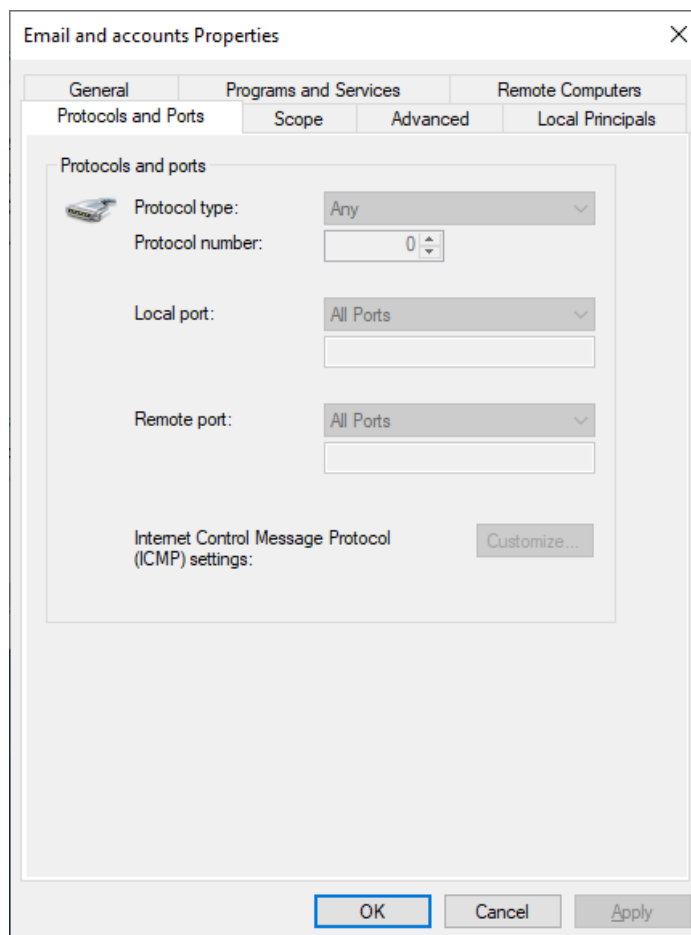
Также как и predetermined rules, these rules cannot be edited.

These rules are assigned to the application package (Application Packages) for the user.



и разрешают для него любой трафик, без ограничений.

Откуда берутся эти правила? Они генерируются приложениями магазина Windows, о чем есть информация в поле Application Package. Сами приложения можно найти в директории C:\Windows\SystemApps.



Для чего нужны эти правила и что будет, если их отключить или удалить? Какого то более менее внятного описания этих правил я не нашел, но если кратко, то они нужны для взаимодействия приложений с внешними сервисами. Например:

- **Work or School account** (Учетная запись для работы или учебы) — обеспечивает связь с учетной записью Azure . Если отключить, учетные записи Azure могут не работать;
- **Your account** (Ваша учетная запись) — обеспечивает связь с облачной службой

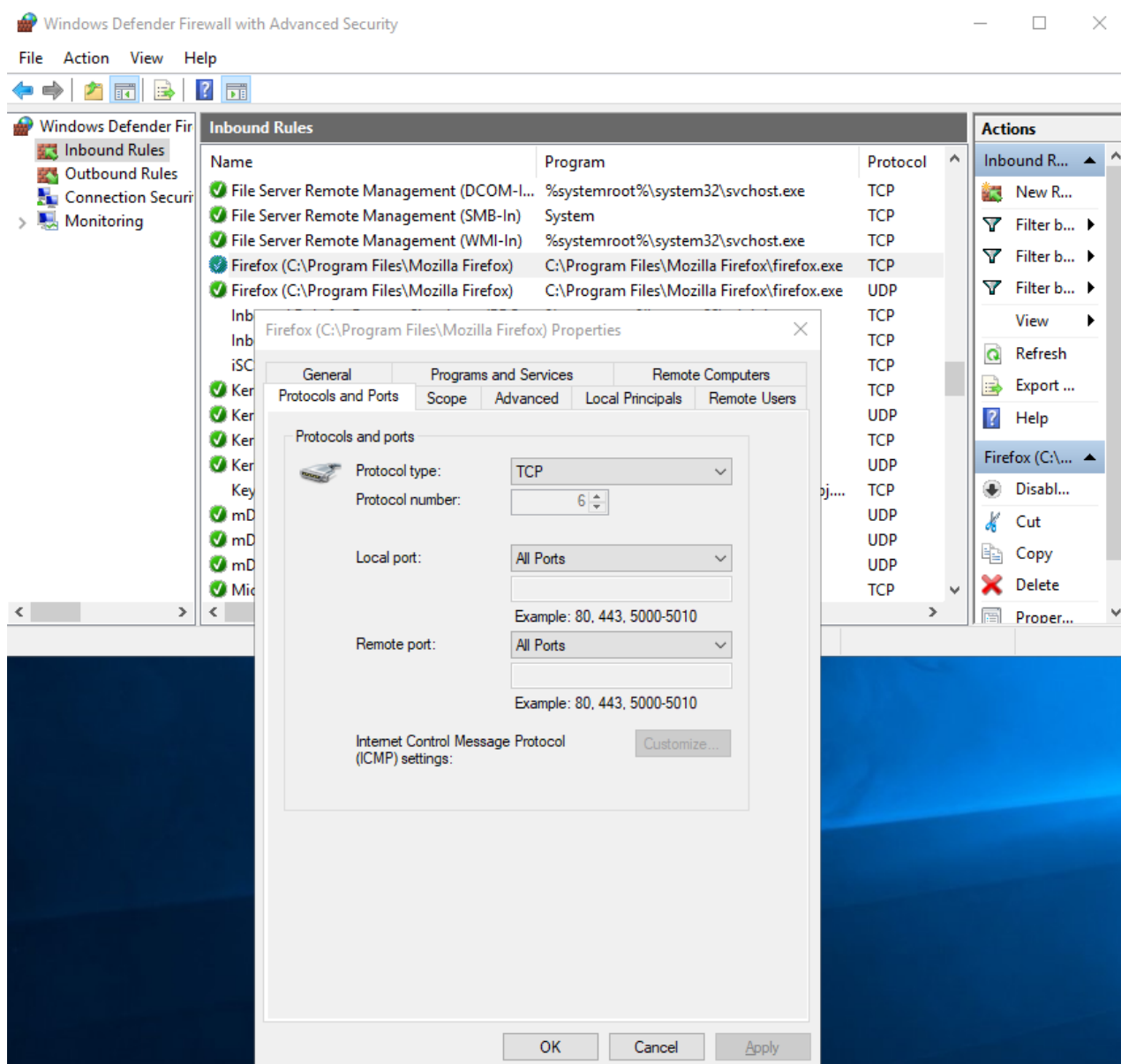
вашей учетной записи Microsoft. Необходимо для настройки синхронизации учетной записи Microsoft между разными компьютерами;

- **Email and accounts** (Электронная почта и учетные записи) — отвечает за синхронизацию учетных записей в приложениях «Почта», «Календарь», «Контакты» и пр.;
- **Cortana** — требуется для работы Cortana, виртуального ассистента для поиска. Cortana использует внешние сервисы, такие как Bing, и при отключении правила поиск может работать некорректно.

Список приложений, и, соответственно, правил может отличаться на разных компьютерах. На вопрос что делать с этими правилами однозначного ответа нет. Оставлять подобные правила, особенно в корпоративной среде, не очень безопасно. Однако эффективных средств борьбы с ними нет, поскольку правила генерируются автоматически для каждого нового пользователя. Такая вот подлянка от Microsoft.

Правила добавляемые при установке приложений

Откуда еще могут появиться правила на фаерволе? Ну например при установке приложений. Для примера установим Firefox и затем обновим список правил. Как видите, добавилось два новых правила для приложения, одно для TCP, второе для UDP. С портами морочиться не стали, разрешили все.



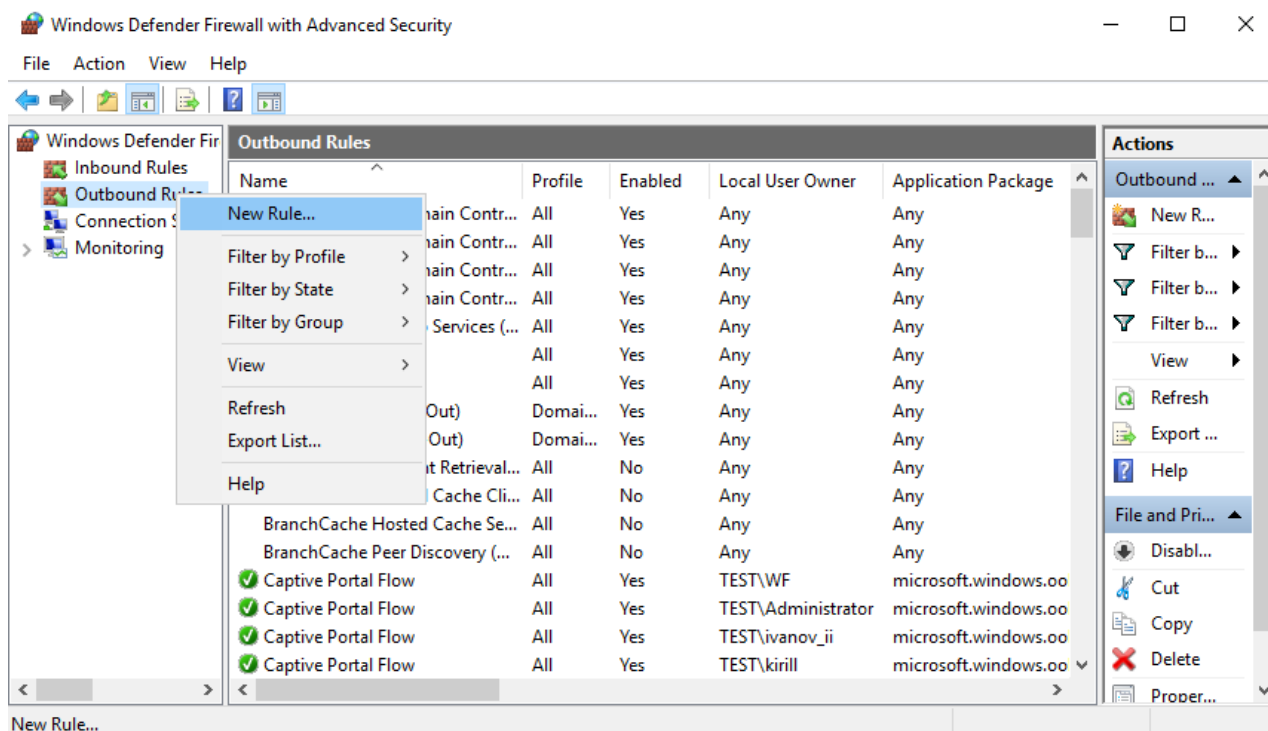
Что интересно, в исходящих правил нет. Т.е. авторы Firefox уверены в том, что весь исходящий трафик не фильтруется. И если ради интереса изменить дефолтное поведение брандмауэра для исходящего трафика и запретить все что не разрешено, то ни один сайт открыть не удастся. Справедливости ради скажу, что это касается не только Firefox, и Chrome и даже встроенный Edge сломаются точно так же.

И если вы захотите контролировать исходящий трафик, то для каждого приложения правила придется создавать вручную. Чем мы и займемся далее.

Правила создаваемые вручную

Для создания правил есть разные способы. Сейчас, для наглядности, воспользуемся графическим интерфейсом. В качестве примера создадим разрешающее правило для исходящего трафика Firefox.

Для создания правила выбираем раздел, кликаем на нем правой клавишей мыши и в контекстном меню выбираем пункт New Rule.



Запускается мастер создания правил, и в первом окне нам надо выбрать тип создаваемого правила. Выбор следующий:

- **Program (Для программы)** — правило, разрешающего или блокирующее весь трафик для конкретного исполняемого файла, независимо от используемых им протоколов и портов;
- **Port (Для порта)** — правило для трафика по определенному TCP или UDP порту, независимо от источника. В одном правиле можно указать одновременно несколько портов;
- **Predefined (Предопределённые)** — здесь мы не создаем новое правило, а выбираем из списка уже имеющих, предопределенных правил;
- **Custom (Настраиваемые)** — универсальный тип правила, в котором можно совместить параметры, например указать и программу, и порт.

Для нашего примера выберем настраиваемое правило.

New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
Active Directory Domain Services
Rule that controls connections for a Windows experience.

☒ **Custom**
Custom rule.

< Back Next > Cancel

Выбираем программу, для которой это правило будет действовать. Мы делаем правило для Firefox, поэтому указываем путь к его исполняемому файлу `firefox.exe`.

New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

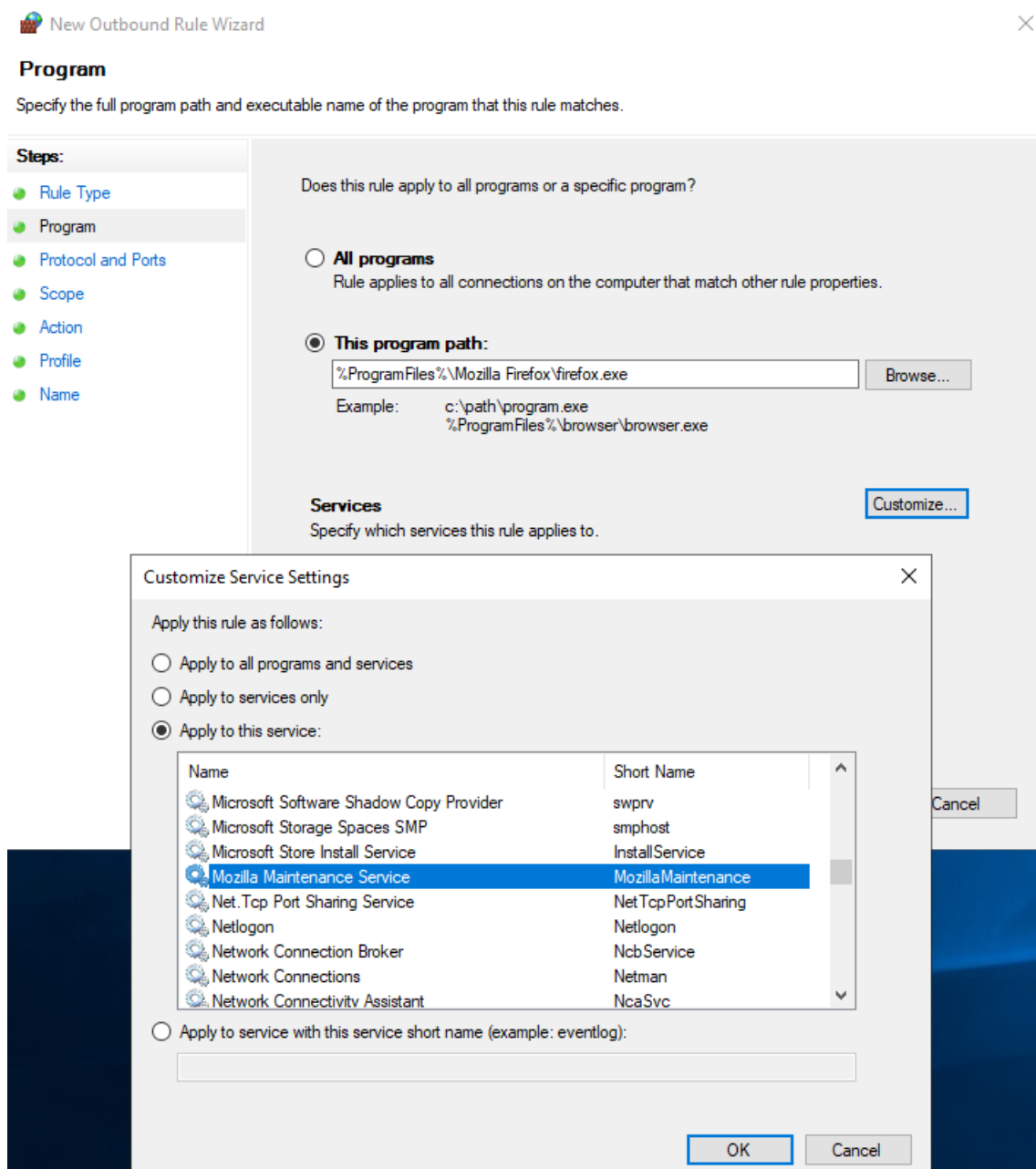
☐ **All programs**
Rule applies to all connections on the computer that match other rule properties.

☒ **This program path:**
%ProgramFiles%\Mozilla Firefox\firefox.exe Browse...
Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

Services Customize...
Specify which services this rule applies to.

< Back Next > Cancel

Не все приложения имеют исполняемый файл, некоторые запускаются в виде сервисов. В этом случае можно по кнопке Customize открыть список имеющихся в смстеме сервисов и выбрать нужный.



В следующем окне указываем протокол и порты, для которых будет работать это правило. Не будем разрешать все, оставим только необходимые для работы браузера порты TCP 80 и 443 (HTTP и HTTPS).

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: Specific Ports

80, 443

Example: 80, 443, 5000-5010

Internet Control Message Protocol
(ICMP) settings:

Customize...

< Back

Next >

Cancel

Дополнительно можно ограничить область действия правила, указав диапазон IP-адресов, как локальных так и удаленных. Например можно разрешить доступ по HTTP только до корпоративных ресурсов.

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- **Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Затем выбираем действие для правила. Всего есть три варианта выбора:

- **Allow the connection** — разрешить подключение.
- **Block the connection** — заблокировать подключение.
- **Allow the connection if it is secure** — разрешить подключение если оно безопасно. В этом случае подключение должно соответствовать правилам безопасности подключения (аутентификация, шифрование и т.п.).

Мы делаем простое разрешающее правило, поэтому выбираем первый пункт.

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- **Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☒ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Customize...

☐ **Block the connection**

< Back

Next >

Cancel

Выбираем сетевые профили, на которые будет распространяться правило.

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- **Profile**
- Name

When does this rule apply?

☒ **Domain**

Applies when a computer is connected to its corporate domain.

☒ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**

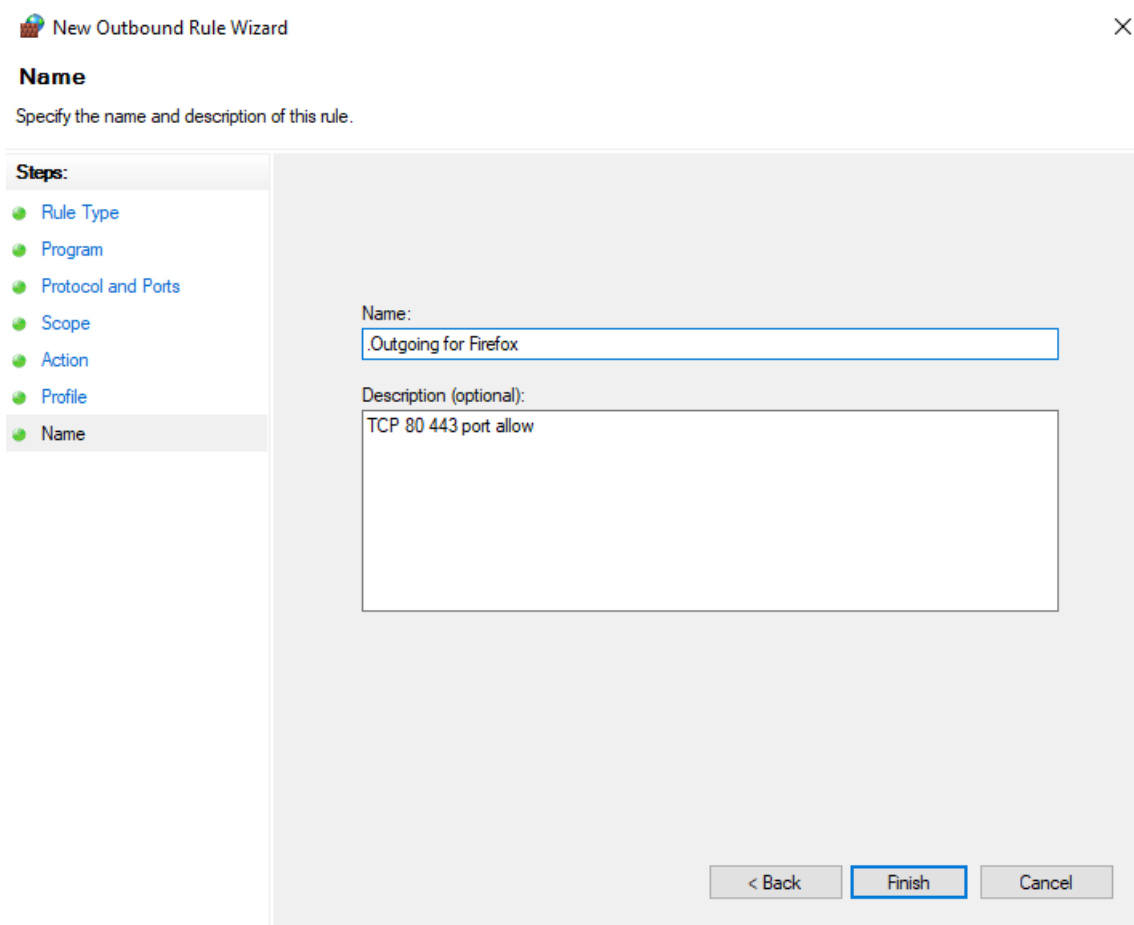
Applies when a computer is connected to a public network location.

< Back

Next >

Cancel

Обзываем правило и сохраняем его. Для того, чтобы правило не потерялось и стояло первым в списке, я обычно ставлю в начале имени точку.



Правила безопасности подключения

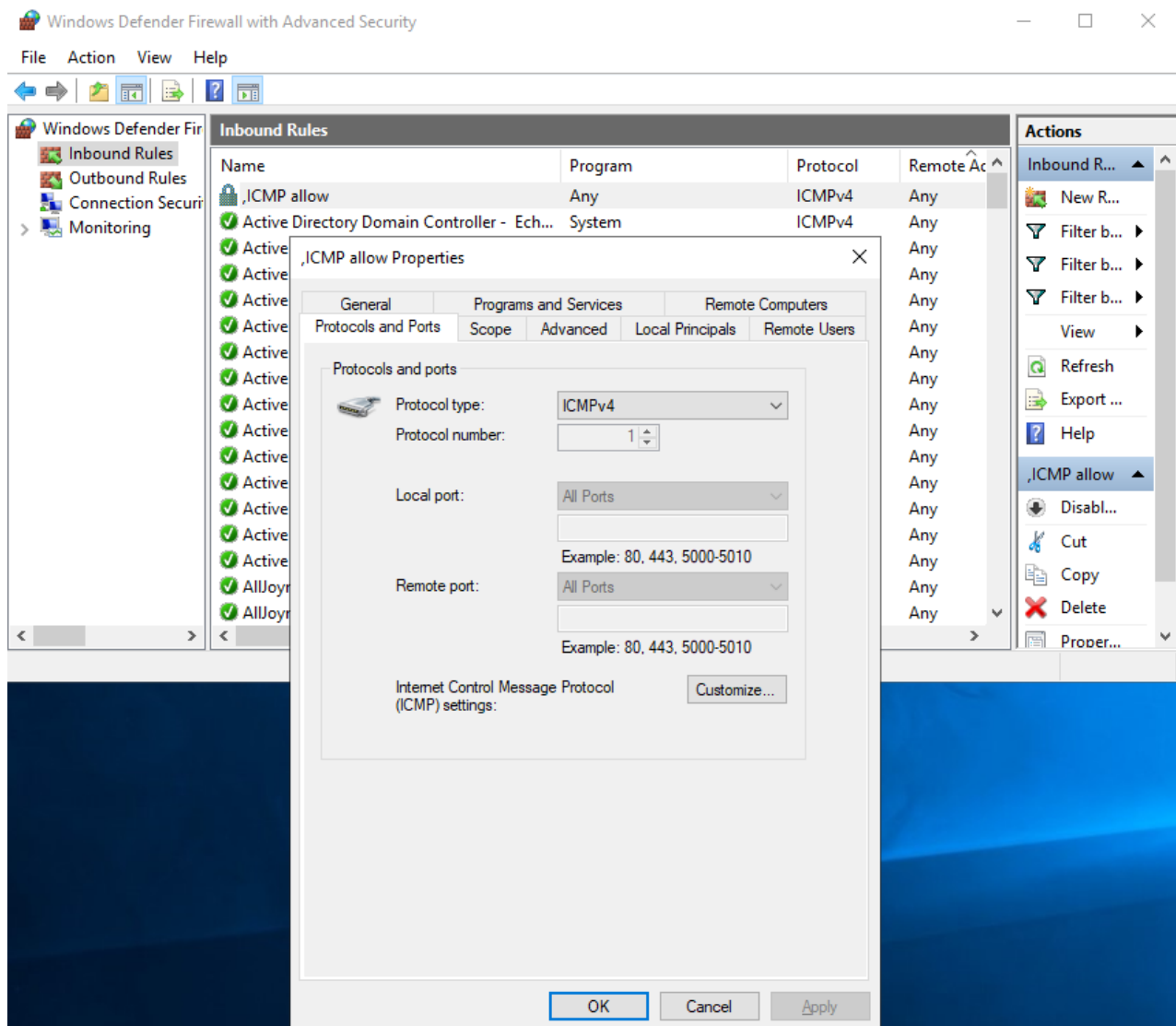
Правила безопасности подключений (Connection security rules) используются для настройки IPSec. При настройке этих правил можно проверять подлинность связи между компьютерами, а затем использовать эту информацию для создания правил брандмауэра на основе определенных учетных записей пользователей и компьютеров.

Правила безопасности подключения не являются самостоятельными правилами, они работают совместно с правилами брандмауэра, дополняя их. Правила брандмауэра разрешают трафик через брандмауэр, но не защищают его. Чтобы защитить трафик с помощью IPsec, необходимо создать правила безопасности подключения. Однако правила безопасности подключения не разрешают трафик через брандмауэр. Для этого требуется создать правило брандмауэра.

Важный момент — правила безопасности подключения не применяются к программам и сервисам. Вместо этого они применяются между компьютерами, составляющими две конечные точки.

А теперь давайте посмотрим, как это выглядит на практике. Для примера возьмем специально созданное правило, разрешающее входящий ICMP-трафик, или, проще говоря, пинг. На данный момент никаких дополнительных ограничений нет и кто

угодно может пинговать наш компьютер.



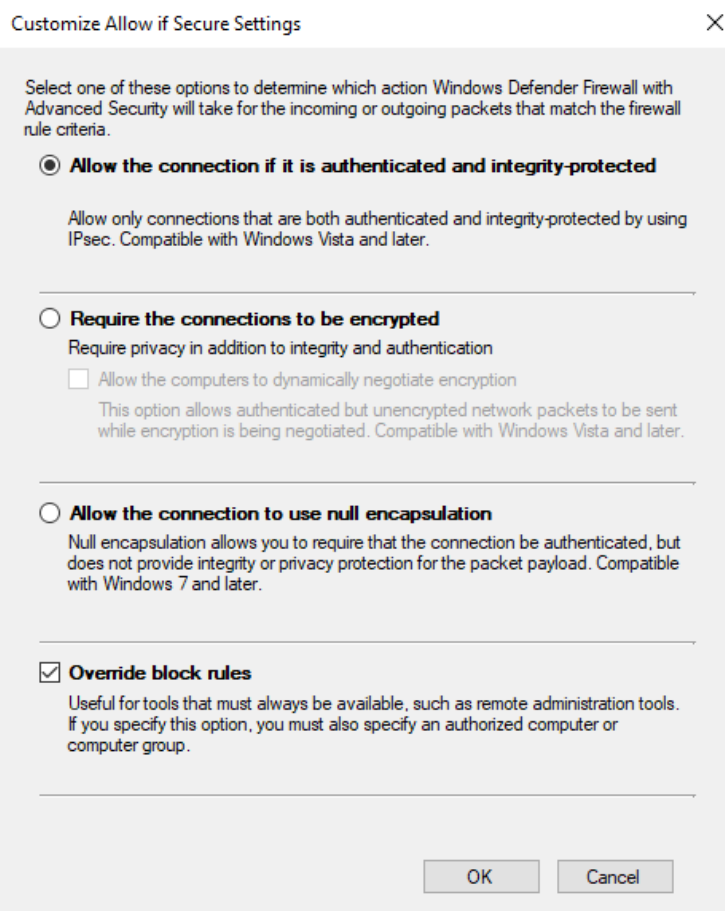
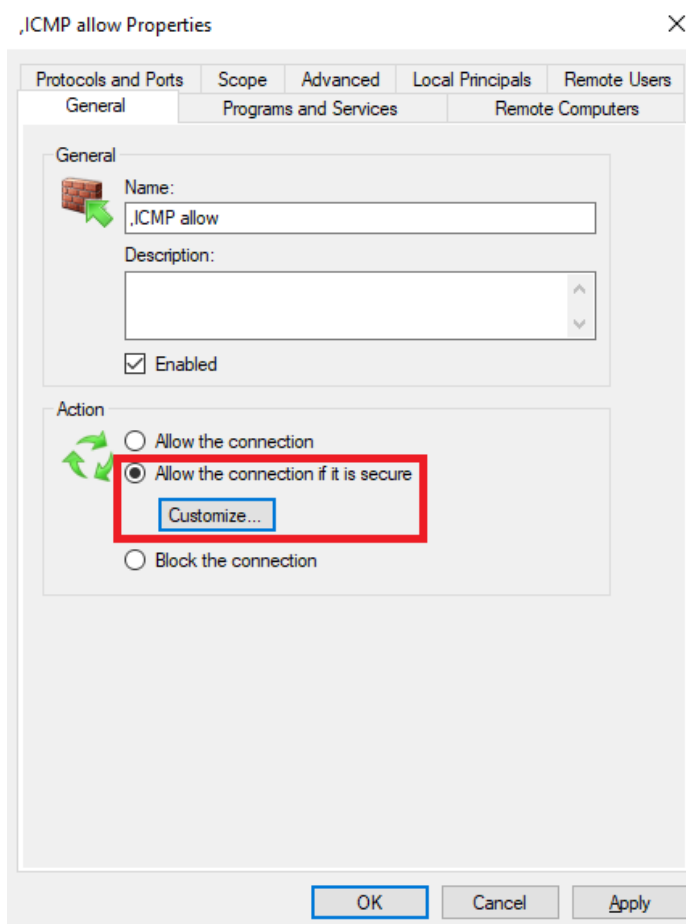
Давайте это изменим и ограничим доступ только определенной группой пользователей и только с определенных компьютеров. Первое, что для этого надо сделать — это изменить действие правила на Allow the connection if it secure (Разрешить только безопасное соединение).

Затем жмем на кнопку Customize и выбираем критерии защищенности подключения:

- **Allow the connection if it is authenticated and integrity-protected** (Разрешать подключения, для которых выполняется проверка подлинности и целостности) — разрешить подключение только в том случае, если оно прошло проверку подлинности (аутентификацию) и целостности с использованием IPsec;
- **Require the connection to be encrypted** (Требовать шифрования подключений) — дополнительно к аутентификации и проверке целостности требуется шифрование;
- **Allow the connection to use null encapsulation** (Разрешить подключению использовать нулевую инкапсуляцию) — нулевая инкапсуляция позволяет требовать для подключения аутентификацию, но не предоставлять проверку целостности и конфиденциальности. Т.е. можно создавать правила безопасности подключения с указанием аутентификации, кроме защиты от пакетов данных

Encapsulating Security Payload (ESP) или Authenticated Header (AH). Эта функция позволяет создать защиту аутентификации в средах с сетевым оборудованием, которое несовместимо с ESP и AH.

Также обратите внимание на чекбокс **Override block rules**. Выше я говорил о том, что запрещающие правила всегда в приоритете над разрешающими. Так вот, этот чекбокс позволяет обойти запрет.

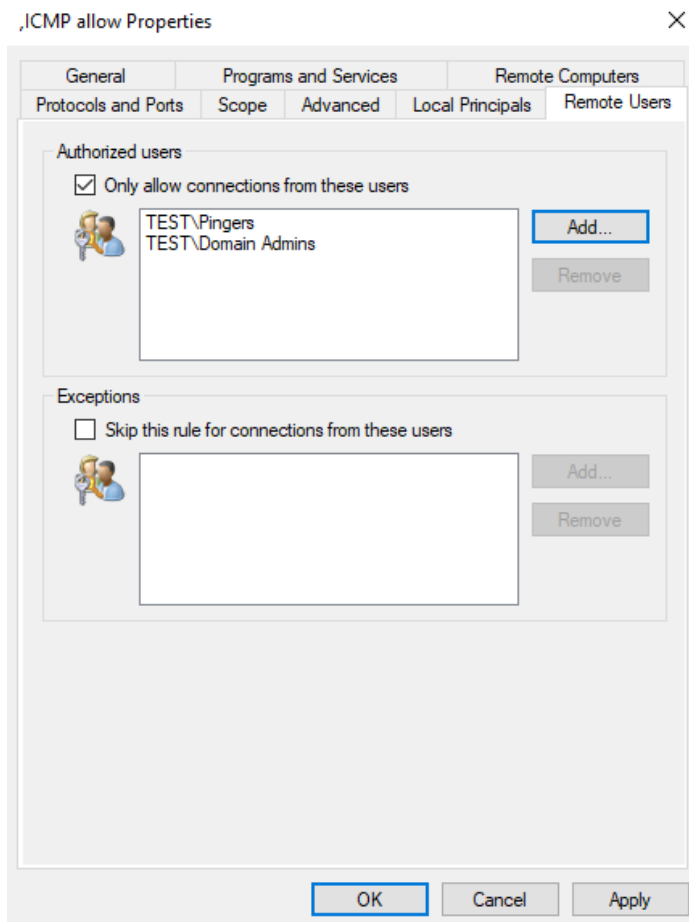


Теперь перейдем на вкладку Remote Users и укажем пользователей, для которых это правило должно работать. Пусть это будут члены доменной группы Pingers и Domain Admins.

Затем перейдем на вкладку Remote Computers и дополнительно укажем компьютер, с которого можно производить подключение. В итоге получается, что сервер смогут пинговать только члены групп Pingers и Domain Admins и только с одного единственного компьютера SRV01.

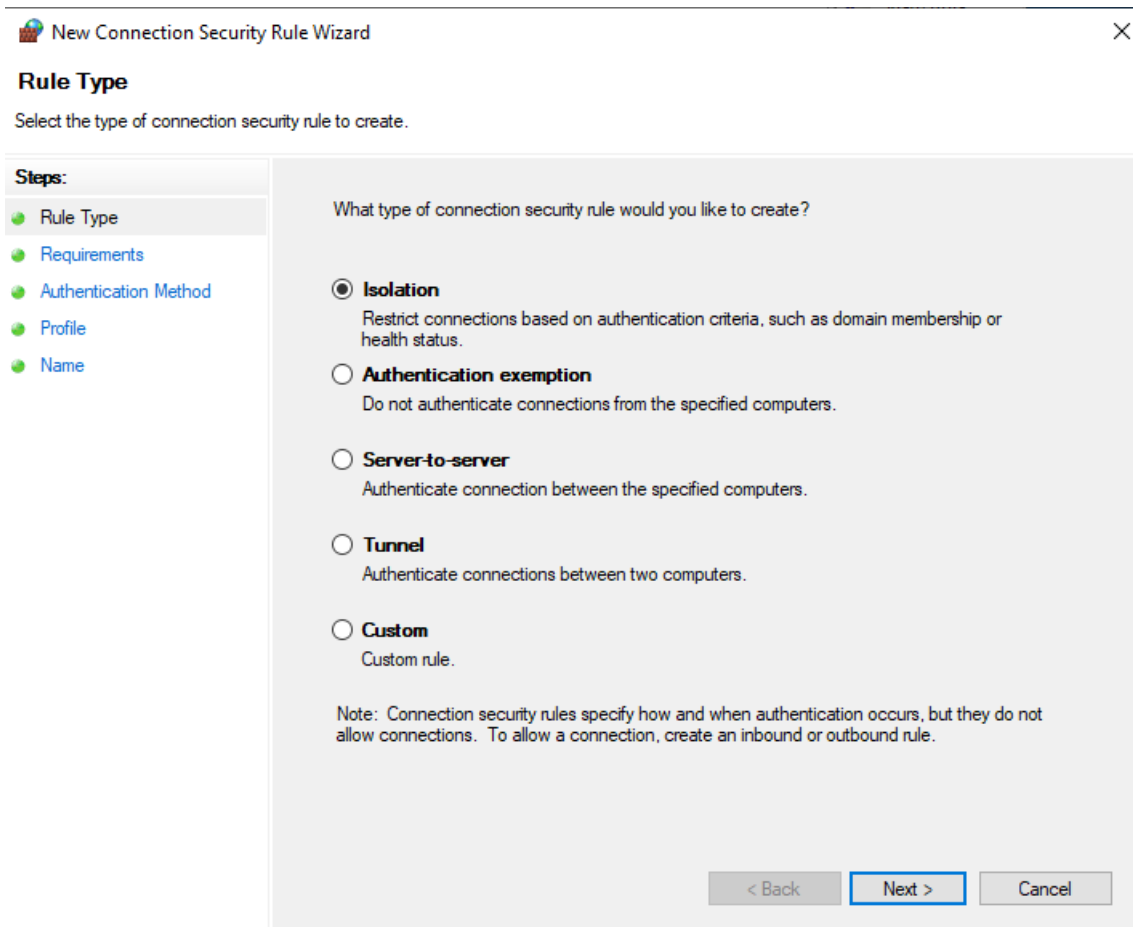
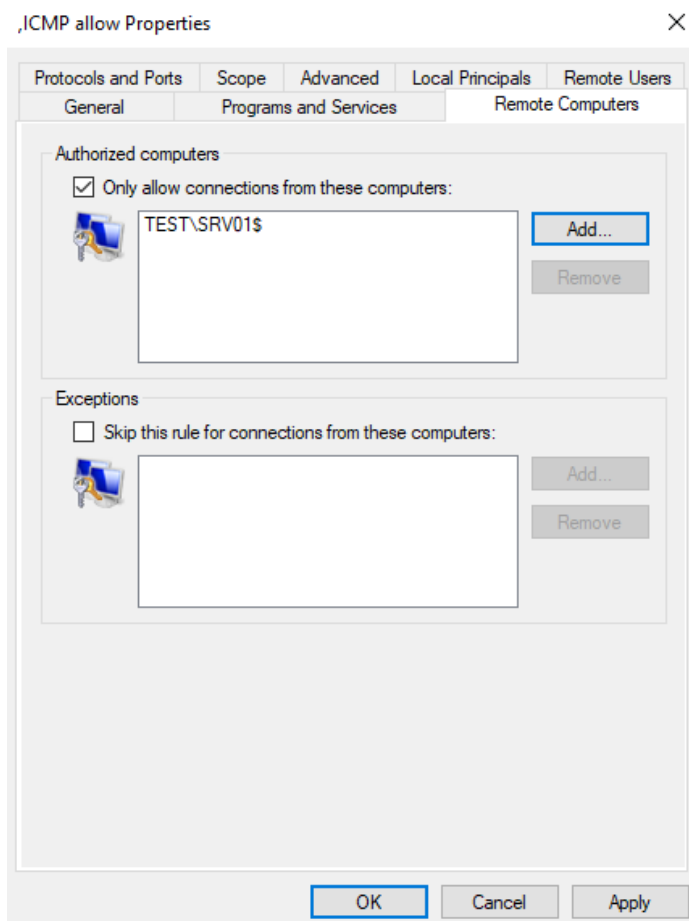
Но это только полдела. Мы создали правило, разрешающее подключение, теперь надо создать правило для его безопасности.

Создаются они так же, как и обычные правила — выбираем раздел, кликаем на нем правой клавишей мыши и в контекстном меню выбираем пункт New Rule. И так же надо выбрать тип создаваемого правила:



- **Isolation** (Изоляция) — изолирует компьютеры, ограничивая подключения на основе учетных данных, таких как членство в домене или состояние работоспособности. Правила изоляции позволяют реализовать стратегию изоляции для отдельных серверов или доменов;
- **Authentication exemption** (Освобождение от аутентификации) — можно использовать, чтобы обозначить соединения, не требующие аутентификации. Можно указывать как назначать компьютеры по определенному IP-адресу, диапазону IP-адресов, подсети или предопределенной группе, например шлюзу;
- **Server to server** (Сервер-сервер) — правило для защиты соединения между конкретными компьютерами. Этот тип правил обычно используют для защиты соединения между серверами. При создании правила указываются конечные точки сети, между которыми защищается связь, а затем требования и аутентификацию, которую необходимо использовать;
- **Tunnel** (Туннель) — позволяет защитить соединения между шлюзами, обычно используется при подключении через Интернет;
- **Custom** (Настраиваемое) — похоже на правило сервер-сервер, но более гибко настраиваемое.

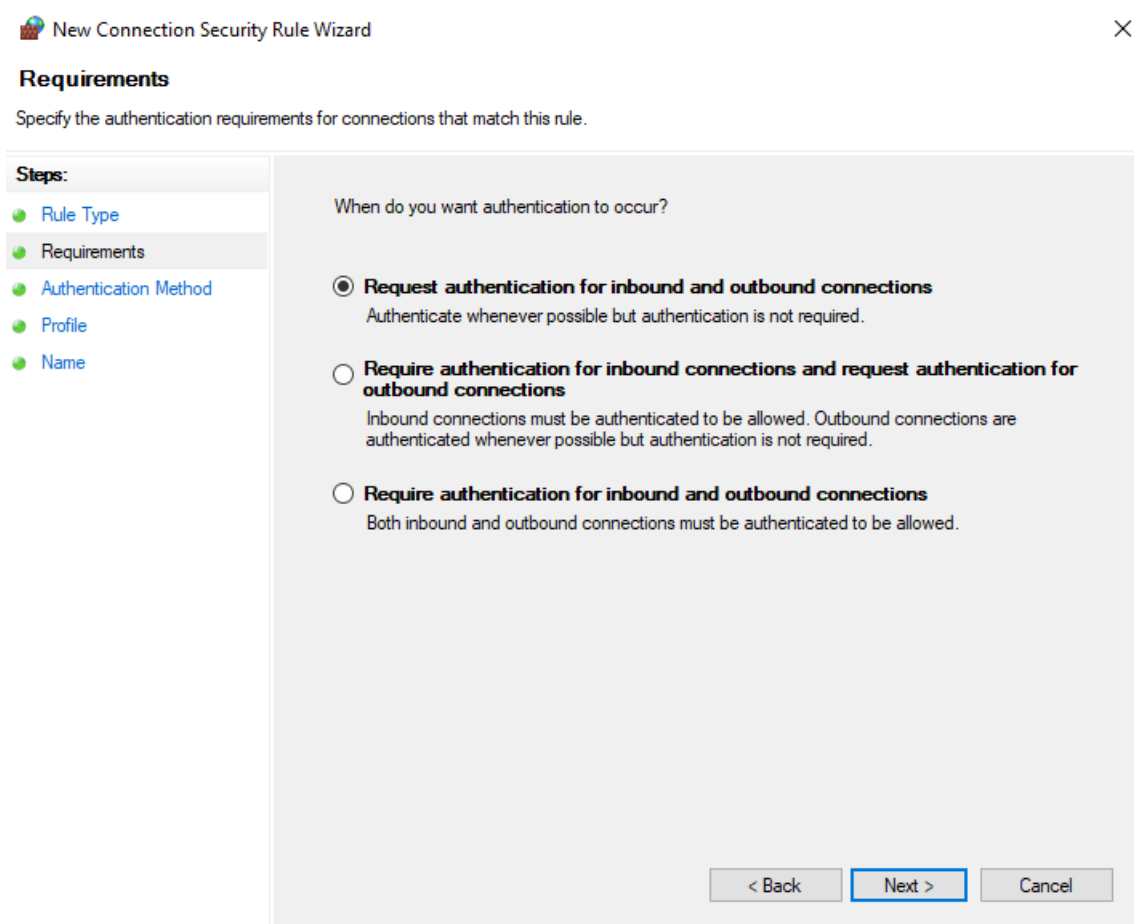
Мы хотим закрыть наш сервер от несанкционированного доступа, поэтому выберем правило изоляции.



На следующем шаге указываем, когда мы хотим производить аутентификацию:

- **Request authentication for inbound and outbound connections option** — запрашивать аутентификацию для входящих и исходящих соединений. При выборе этого варианта мы указываем, что весь входящий и исходящий трафик должен проходить проверку подлинности, но соединение будет разрешено в любом случае. Однако если аутентификация прошла успешно, трафик будет защищен;
- **Require authentication for inbound connections and Request authentication for outbound connections option** — требовать аутентификацию для входящих подключений и запрашивать аутентификацию для исходящих подключений. Это гарантирует, что весь входящий трафик пройдет аутентификацию либо будет заблокирован. При этом исходящий трафик, для которого не удалось выполнить аутентификацию, будет разрешен;
- **Require authentication for inbound and outbound connections option** — требовать аутентификацию для входящих и исходящих соединений. Самый жесткий вариант, при котором весь входящий и исходящий трафик либо аутентифицируется, либо блокируется.

Для нашего примера выберем первый вариант.



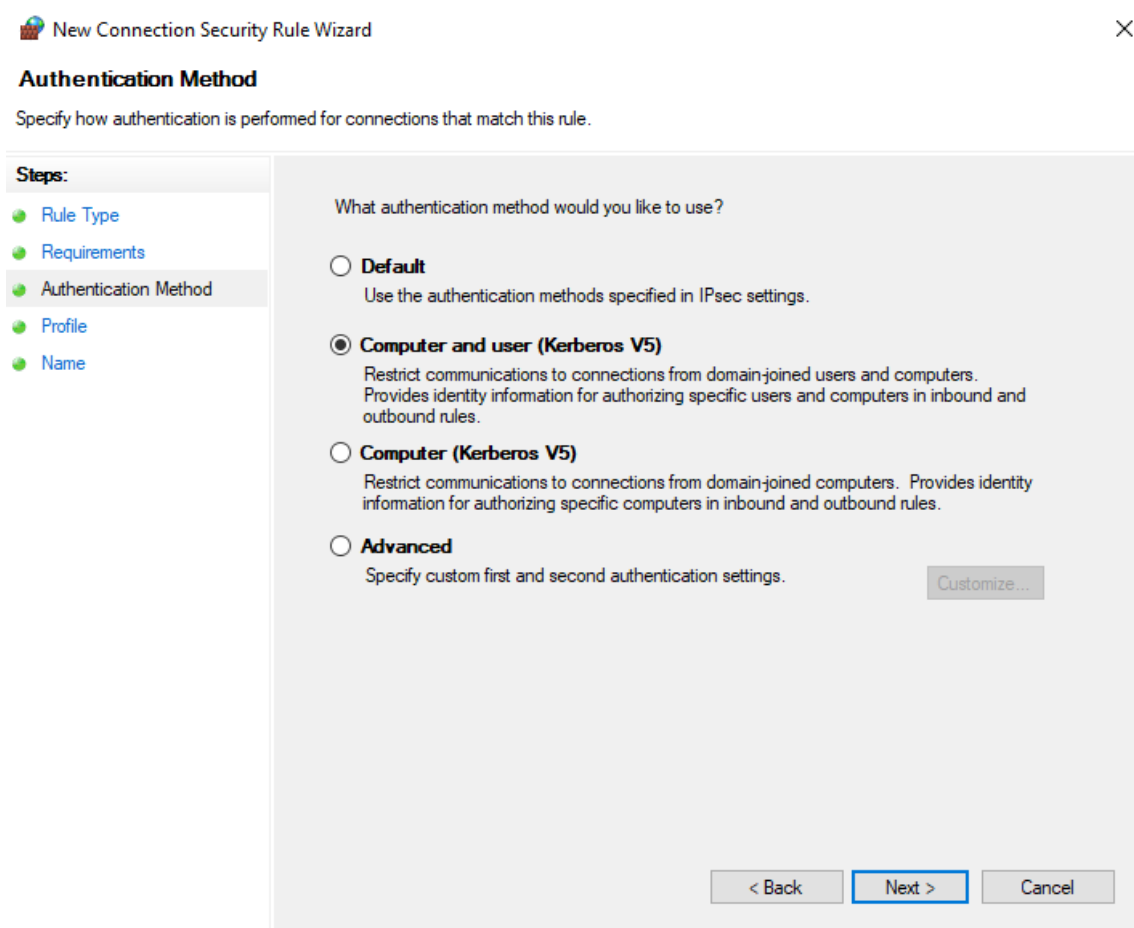
Затем выбираем метод аутентификации:

- **Default** — использовать метод аутентификации, настроенный на вкладке «Параметры IPsec» свойств фаервола;
- **Computer and user (Kerberos V5)** — метод «Компьютер и пользователь» (Kerberos V5) использует аутентификацию как компьютера, так и пользователя. Это

означает, что можно запросить или потребовать аутентификацию как пользователя, так и компьютера, прежде чем продолжить обмен данными. Напомню, что использовать протокол аутентификации Kerberos V5 можно только в том случае, только если оба компьютера являются членами домена;

- **Computer (Kerberos V5)** — метод «Компьютер» (Kerberos V5) запрашивает или требует от компьютера пройти проверку подлинности с использованием протокола проверки подлинности Kerberos V5;
- **User (Kerberos V5)** — метод User (Kerberos V5) запрашивает или требует от пользователя пройти проверку подлинности с использованием протокола проверки подлинности Kerberos V5;
- **Advanced** — расширенный. Здесь вы можете настроить любой доступный метод. Можно выбрать не только Kerberos V5, но и NTLM V2, сертификаты и даже общий ключ (для компьютера). Также можно указывать первый и второй метод аутентификации, отдельно для компьютера и для пользователя.

Мы планируем аутентифицировать и компьютер и пользователя, поэтому выбираем второй пункт.



Ну и дальше все как обычно — отмечаем профили

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

When does this rule apply?

☒ **Domain**

Applies when a computer is connected to its corporate domain.

☒ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**

Applies when a computer is connected to a public network location.

< Back

Next >

Cancel

даем правилу имя и сохраняем его.

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

Name:

Description (optional):

< Back

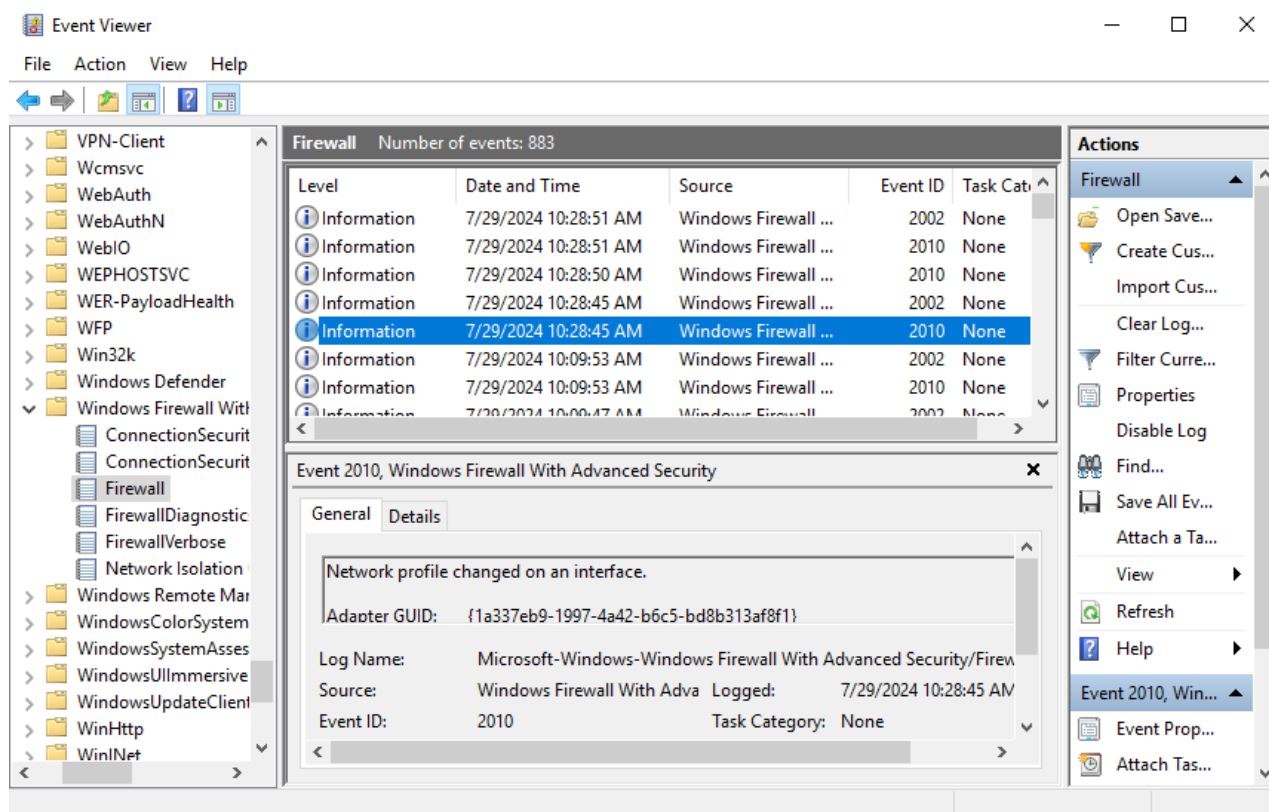
Finish

Cancel

Теперь дело сделано. Мы создали правило безопасности, в котором описали, какое именно подключение считается защищенным. И правило фаервола сработает только для такого трафика.

Логирование

Начиная с Windows 7 и Windows Server 2008 R2 события брандмауэра Windows, такие как изменение настроек, создание правил и т.п., пишутся в отдельный журнал **Event Viewer\Application and Services Logs\Microsoft\Windows\Windows Firewall with Advanced Security**.



Также у фаервола есть собственный журнал, куда пишутся все попытки подключения. По умолчанию он отключен, и включают его при настройке и отладке правил, либо при наличии проблем с подключением. Включить его можно в свойствах фаервола, в разделе **Logging** нажав кнопку **Customize**.

Можно указать путь, по которому будут находиться файлы журнала, задать максимальный размер файла и выбрать, что должно логироваться — неудачные попытки (dropped packets), успешные подключения (successful connection) или и то и другое. Как правило, для диагностики достаточно логировать только ошибки.

Сам журнал представляет из себя обычный текстовый файл с набором полей — время, действие, протокол, порт, адрес клиента и направление трафика. Информации не особо много, но вполне достаточно для диагностики.

Domain Profile Private Profile Public Profile IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended) ▾

Inbound connections: Block (default) ▾

Outbound connections: Block ▾

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

OK Cancel Apply

Name: .\system32\LogFiles\Firewall\pfirewall.log Browse...

Size limit (KB): 4,096 ▴ ▾

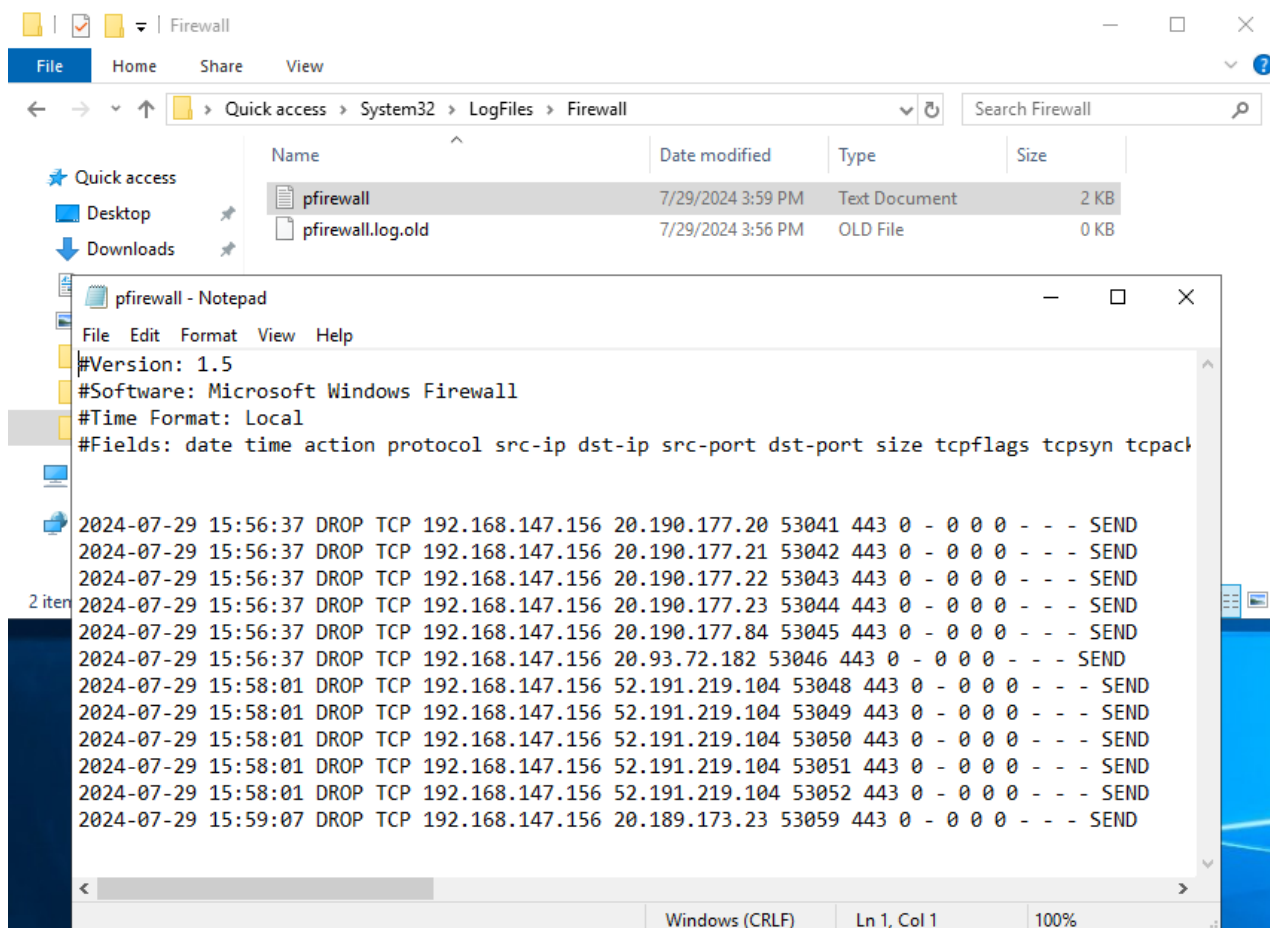
Log dropped packets: Yes ▾

Log successful connections: No (default) ▾

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

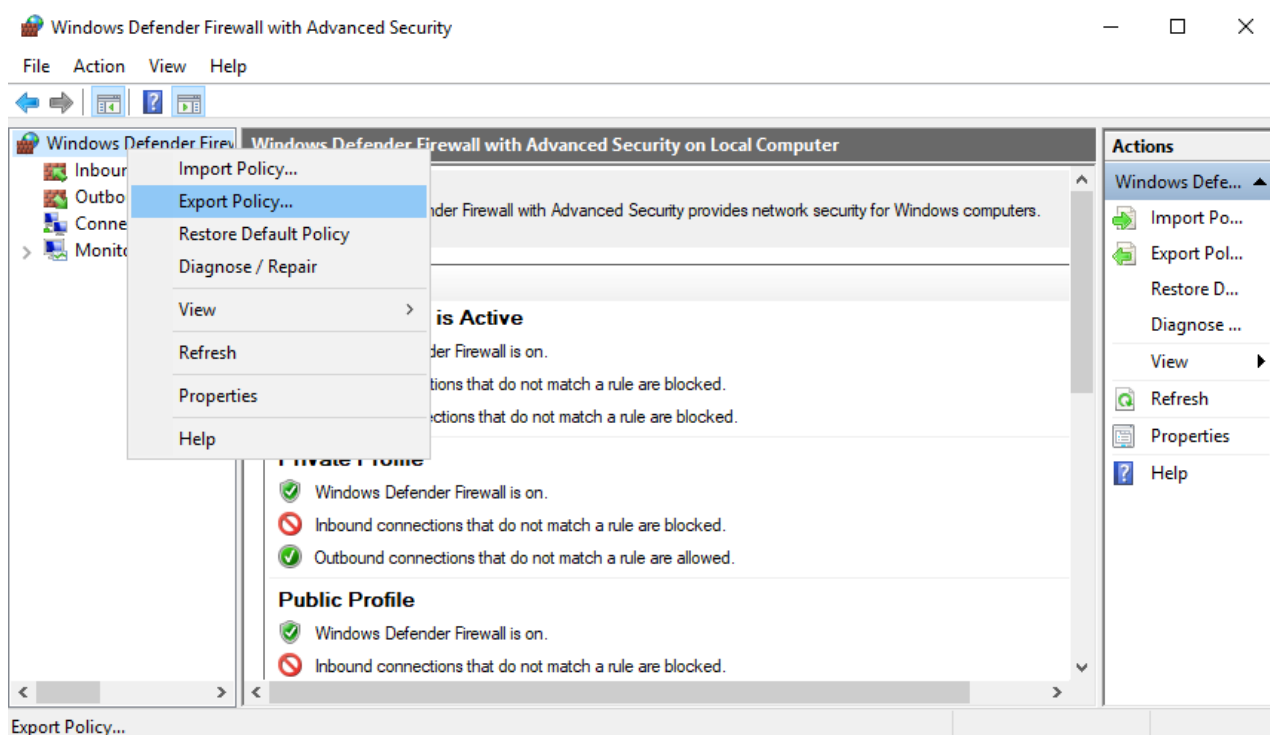
Default path for the log file is
%systemroot%\system32\logfiles\Firewall\pfirewall.log.

OK Cancel



Экспорт, импорт и сброс настроек

Все настройки и созданные правила можно импортировать в файл. Этот файл затем можно использовать для импорта настроек на этот же или любой другой компьютер. Также можно сбросить все настройки к первоначальному состоянию, которое было сразу после установки операционной системы.

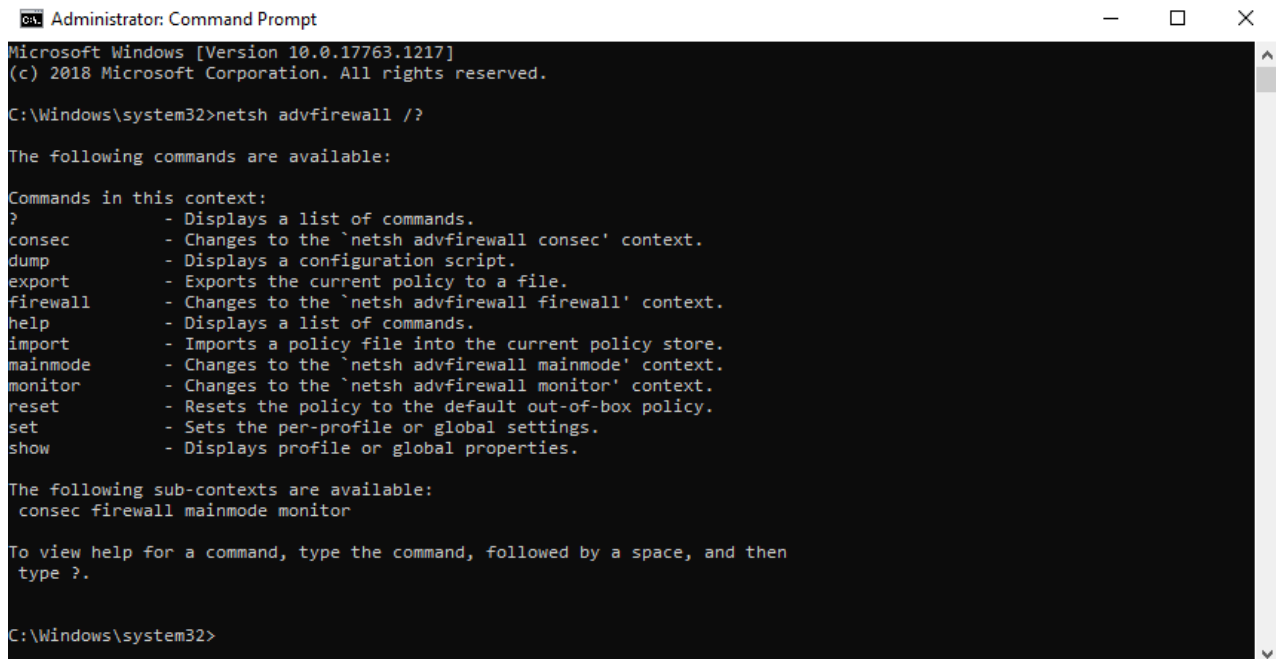


Управление фаерволом с помощью утилиты netsh

Кроме стандартной оснастки управлять настройками фаервола можно и другими средствами. Самое старое и проверенное — это утилита командной строки **netsh**. Не смотря на свой почтенный возраст очень мощный инструмент для управления сетью, который в числе прочего умеет работать и с фаерволом.

Посмотреть, что нам предлагает netsh для фаервола можно командой:

```
netsh advfirewall /?
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh advfirewall /?

The following commands are available:

Commands in this context:
?                - Displays a list of commands.
consec           - Changes to the 'netsh advfirewall consec' context.
dump            - Displays a configuration script.
export          - Exports the current policy to a file.
firewall        - Changes to the 'netsh advfirewall firewall' context.
help            - Displays a list of commands.
import          - Imports a policy file into the current policy store.
mainmode        - Changes to the 'netsh advfirewall mainmode' context.
monitor         - Changes to the 'netsh advfirewall monitor' context.
reset           - Resets the policy to the default out-of-box policy.
set             - Sets the per-profile or global settings.
show            - Displays profile or global properties.

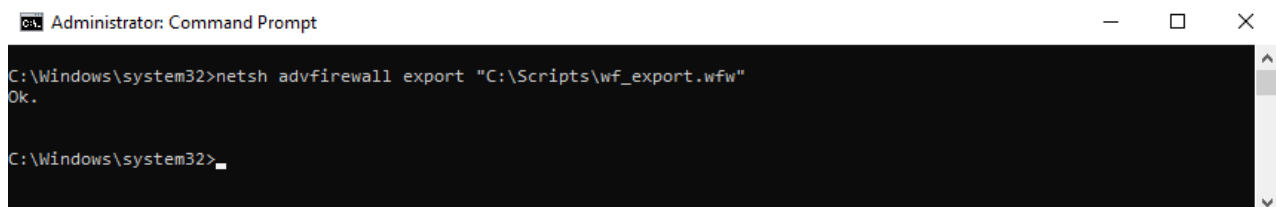
The following sub-contexts are available:
consec firewall mainmode monitor

To view help for a command, type the command, followed by a space, and then
type ?.

C:\Windows\system32>
```

Для начала произведем экспорт настроек командой:

```
netsh advfirewall export "C:\Scripts\wf_export.wfw"
```



```
Administrator: Command Prompt

C:\Windows\system32>netsh advfirewall export "C:\Scripts\wf_export.wfw"
Ok.

C:\Windows\system32>
```

Затем изменим действия по умолчанию для активного профиля, разрешим исходящий трафик:

```
netsh advfirewall set currentprofile firewallpolicy
blockinbound,allowoutbound
```

И выведем текущие настройки:

```
netsh advfirewall show domainprofile
```

```
Select Administrator: Command Prompt

C:\Windows\system32>netsh advfirewall set currentprofile firewallpolicy blockinbound,allowoutbound
Ok.

C:\Windows\system32>netsh advfirewall show domainprofile

Domain Profile Settings:
-----
State                               ON
Firewall Policy                     BlockInbound,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification             Disable
RemoteManagement                   Disable
UnicastResponseToMulticast          Enable

Logging:
LogAllowedConnections               Disable
LogDroppedConnections               Enable
FileName                            %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                          4096

Ok.

C:\Windows\system32>
```

Теперь создадим новое правило для входящих подключений, запрещающее TCP-трафик по 80 порту, назовем его nohttp:

```
netsh advfirewall firewall add rule name="nohttp" protocol=TCP localport=80
action=block dir=IN
```

И проверим что получилось:

```
netsh advfirewall firewall show rule name="nohttp"
```

```
Administrator: Command Prompt

C:\Windows\system32>netsh advfirewall firewall add rule name="nohttp" protocol=TCP localport=80 action=block dir=IN
Ok.

C:\Windows\system32>netsh advfirewall firewall show rule name="nohttp"

Rule Name:                          nohttp
-----
Enabled:                             Yes
Direction:                           In
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                             Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                             80
RemotePort:                           Any
Edge traversal:                         No
Action:                               Block
Ok.

C:\Windows\system32>
```

Управление фаерволом с помощью PowerShell

Переходим к более современным средствам управления, таким как PowerShell. Для управления фаерволом в нем есть отдельный модуль NetSecurity. Посмотреть список командлетов в модуле можно командой:

```
Get-Command -Module NetSecurity
```

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-Command -Module NetSecurity

CommandType      Name                                     Version      Source
-----
Function         Copy-NetFirewallRule                   2.0.0.0     NetSecurity
Function         Copy-NetIPsecMainModeCryptoSet         2.0.0.0     NetSecurity
Function         Copy-NetIPsecMainModeRule              2.0.0.0     NetSecurity
Function         Copy-NetIPsecPhase1AuthSet             2.0.0.0     NetSecurity
Function         Copy-NetIPsecPhase2AuthSet             2.0.0.0     NetSecurity
Function         Copy-NetIPsecQuickModeCryptoSet        2.0.0.0     NetSecurity
Function         Copy-NetIPsecRule                      2.0.0.0     NetSecurity
Function         Disable-NetFirewallRule                2.0.0.0     NetSecurity
Function         Disable-NetIPsecMainModeRule           2.0.0.0     NetSecurity
Function         Disable-NetIPsecRule                   2.0.0.0     NetSecurity
Function         Enable-NetFirewallRule                 2.0.0.0     NetSecurity
Function         Enable-NetIPsecMainModeRule            2.0.0.0     NetSecurity
Function         Enable-NetIPsecRule                    2.0.0.0     NetSecurity
Function         Find-NetIPsecRule                      2.0.0.0     NetSecurity
Function         Get-NetFirewallAddressFilter            2.0.0.0     NetSecurity
Function         Get-NetFirewallApplicationFilter        2.0.0.0     NetSecurity
Function         Get-NetFirewallInterfaceFilter          2.0.0.0     NetSecurity
Function         Get-NetFirewallInterfaceTypeFilter      2.0.0.0     NetSecurity
```

Продолжим начатое дело 😊 и выведем и выведем информацию о созданном ранее правиле:

```
Get-NetFirewallRule -DisplayName "nohttp"
```

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "nohttp"

Name                : {B1C92147-F053-4D50-B314-828B2FFF89E3}
DisplayName          : nohttp
Description          :
DisplayGroup        :
Group                :
Enabled              : True
Profile              : Any
Platform             : {}
Direction            : Inbound
Action               : Block
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner                :
PrimaryStatus        : OK
Status               : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local

PS C:\Windows\system32>
```

PowerShell в отличие от netsh не выводит одним командлетом всю информацию о правиле. Так если мы хотим посмотреть настройки фильтра для порта, то надо будет использовать командлет Get-NetFirewallPortFilter, например так:

```
Get-NetFirewallRule -DisplayName "nohttp" | Get-NetFirewallPortFilter
```

А если мы захотим изменить настройки фильтра для правила, например запретить 443 порт, то получится вот такая конструкция:

```
Get-NetFirewallRule -DisplayName "nohttp" | Get-NetFirewallPortFilter |
Set-NetFirewallPortFilter -LocalPort 80,443
```



```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "nohttp" | Get-NetFirewallPortFilter

Protocol      : TCP
LocalPort     : 80
RemotePort    : Any
IcmpType      : Any
DynamicTarget : Any

PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "nohttp" | Get-NetFirewallPortFilter | Set-NetFirewallPortFilter
-LocalPort 80,443
PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "nohttp" | Get-NetFirewallPortFilter

Protocol      : TCP
LocalPort     : {80, 443}
RemotePort    : Any
IcmpType      : Any
DynamicTarget : Any
```

Ну и завершим издевательства над правилом, переименовав его в nohttphttps:

```
Get-NetFirewallRule -DisplayName "nohttp" | Set-NetFirewallRule -
NewDisplayName "nohttphttps"
```

Проверим результат:

```
Get-NetFirewallRule -DisplayName "nohttphttps"
```

и удалим злосчастное правило:

```
Remove-NetFirewallRule -DisplayName "nohttphttps"
```

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "nohttp" | Set-NetFirewallRule -NewDisplayName "nohttphttps"
PS C:\Windows\system32> Get-NetFirewallRule -DisplayName "nohttphttps"

Name                : {B1C92147-F053-4D50-B314-828B2FFB9E3}
DisplayName          : nohttphttps
Description          :
DisplayGroup        :
Group               :
Enabled              : True
Profile             : Any
Platform            : {}
Direction           : Inbound
Action              : Block
EdgeTraversalPolicy  : Block
LooseSourceMapping   : False
LocalOnlyMapping     : False
Owner               :
PrimaryStatus        : OK
Status              : The rule was parsed successfully from the store. (65536)
EnforcementStatus    : NotApplicable
PolicyStoreSource    : PersistentStore
PolicyStoreSourceType : Local

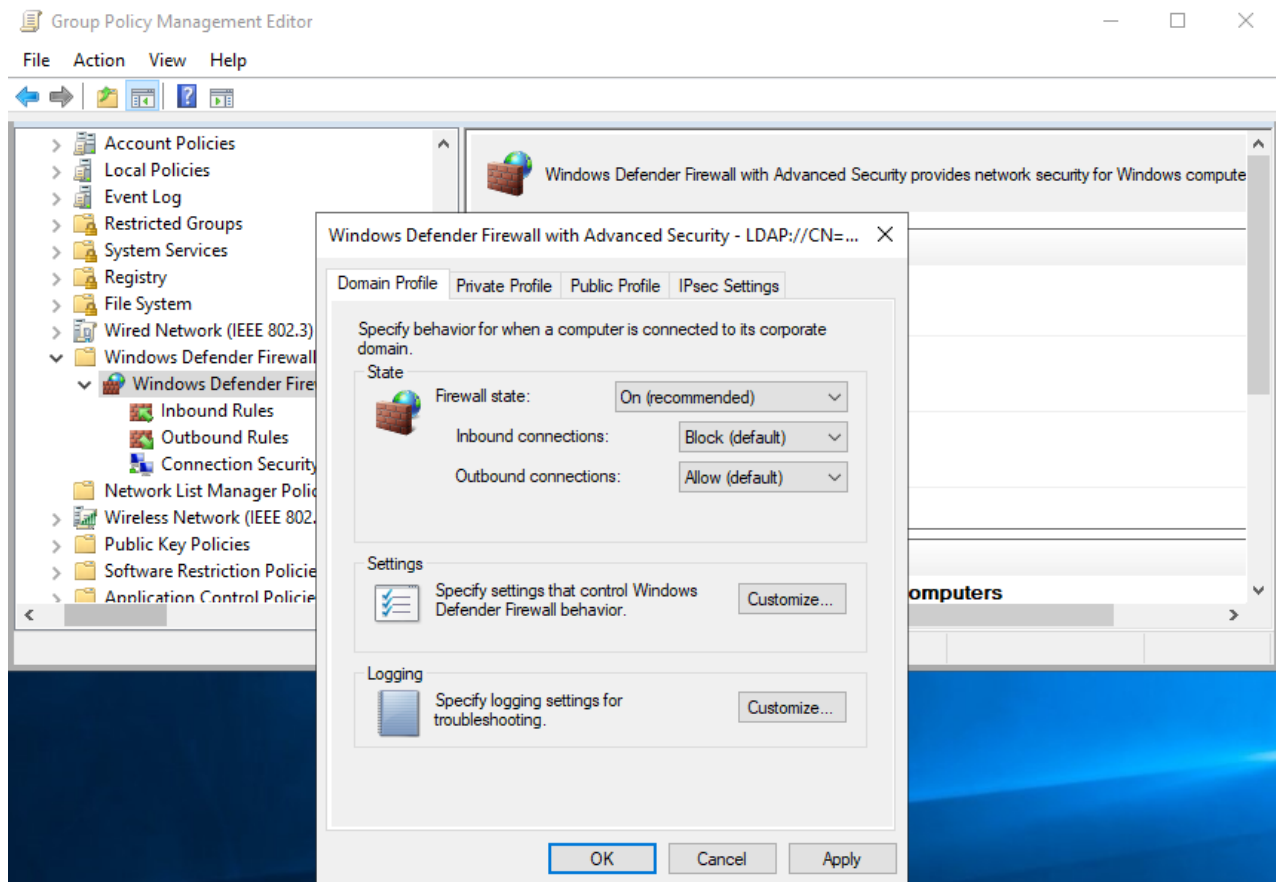
PS C:\Windows\system32> Remove-NetFirewallRule -DisplayName "nohttphttps"
PS C:\Windows\system32>
```

Управление фаерволом с помощью групповых политик

Ну и самый мощный инструмент, с помощью которого можно централизованно распространять настройки фаервола на все компьютеры организации. Раздел с настройками находится в **Computer Configuration > Policies > Windows Settings >**

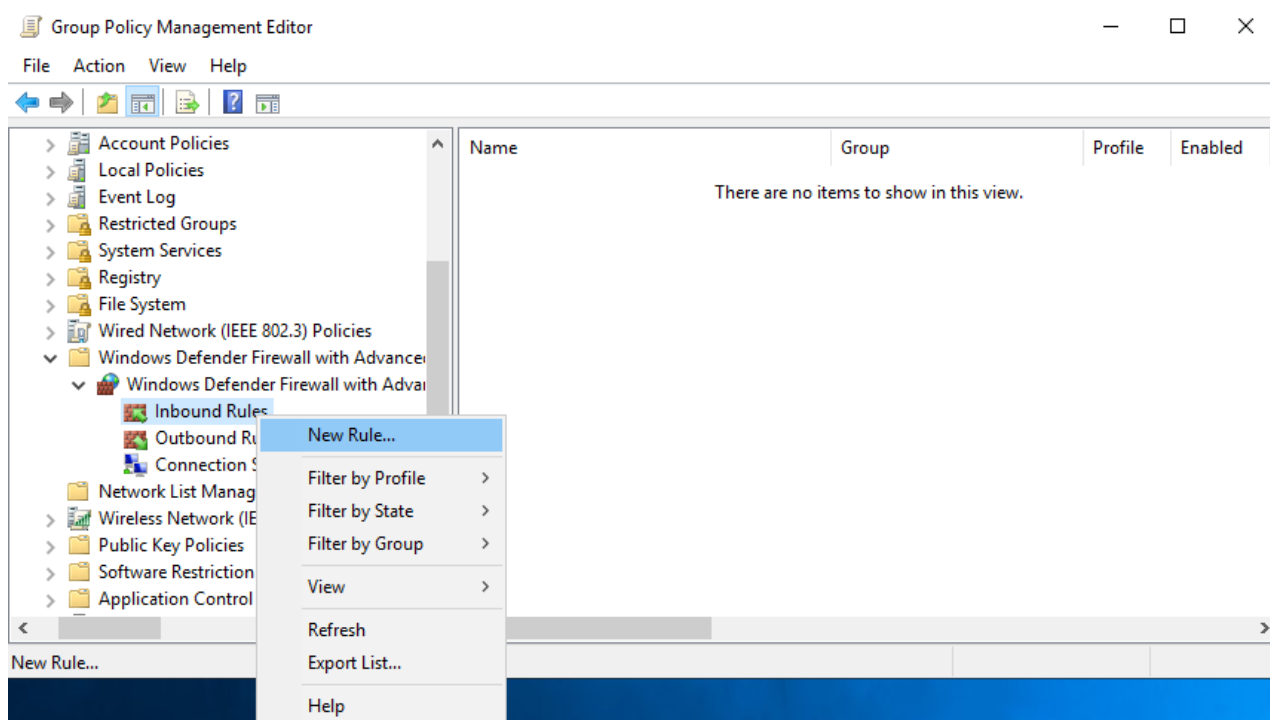
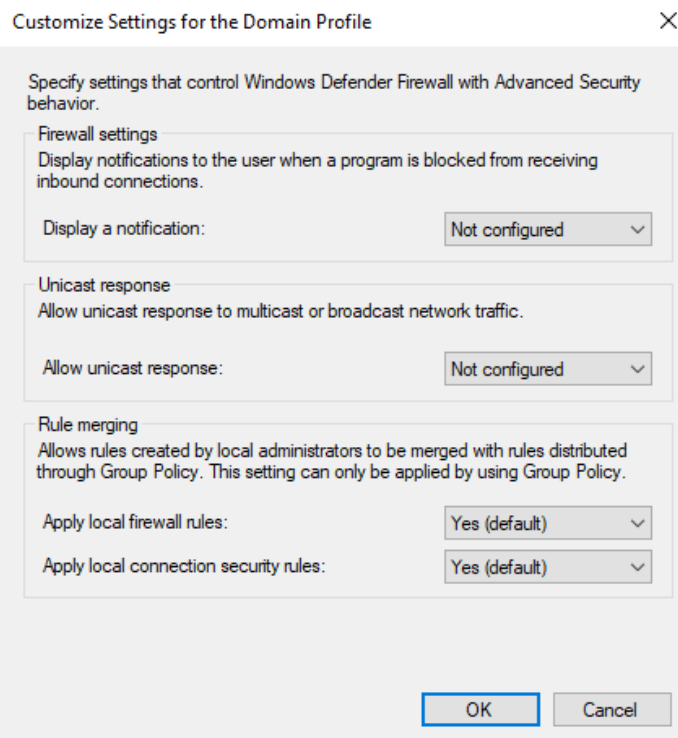
Security Settings > Windows Defender Firewall with Advanced Security.

Окно настроек выглядит так же, как и у локальной консоли. Здесь можно так же установить состояние фаервола и указать действия по умолчанию.

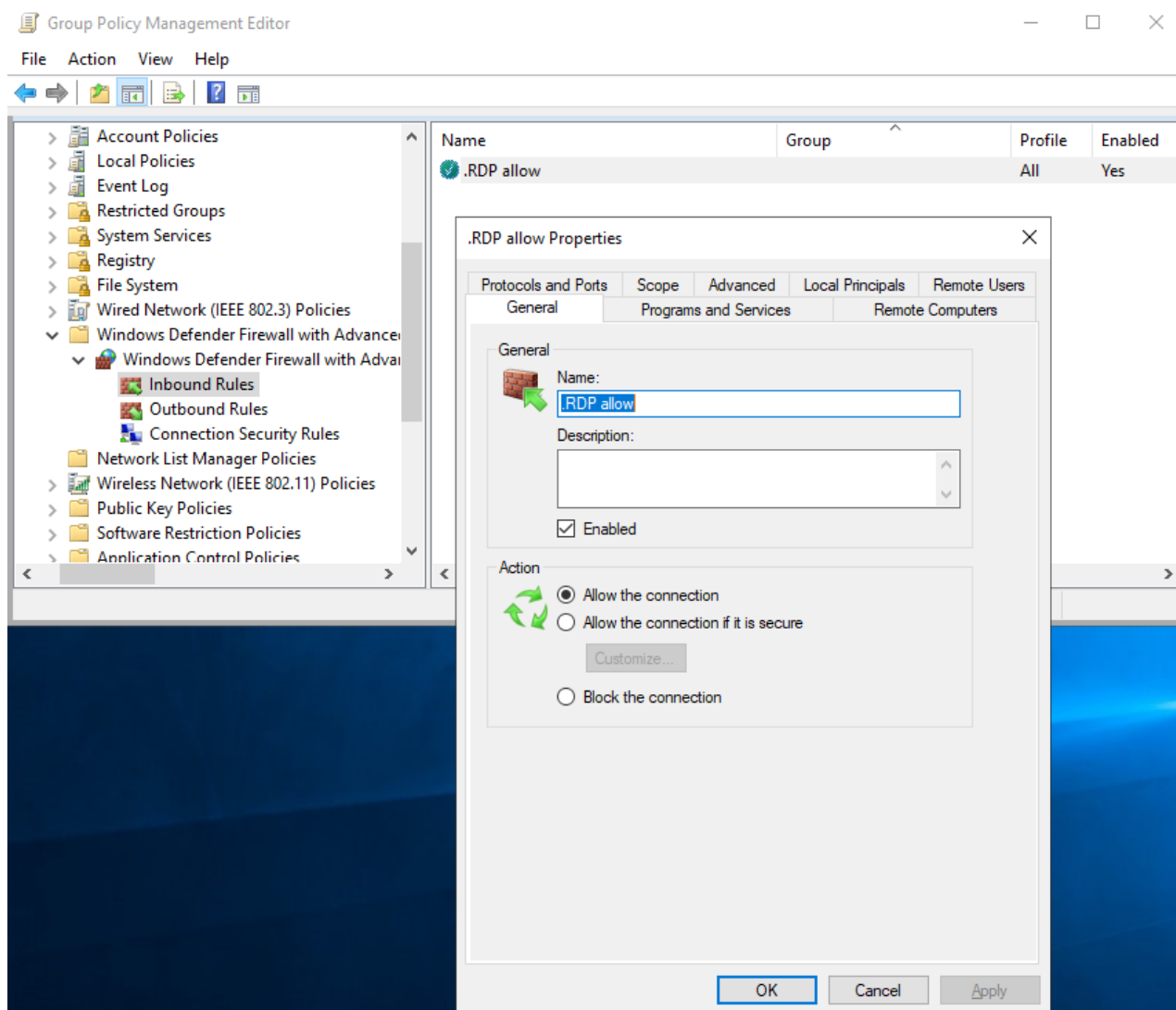


Дополнительно можно настроить взаимодействие локальных правил с правилами, назначенными групповой политикой. Для этого надо нажать кнопку **Customize** в поле **Settings**, и в открывшемся окне в поле **Rule merging** выбрать варианты слияния. По умолчанию локальные правила разрешены и обрабатываются вместе с правилами из групповой политики.

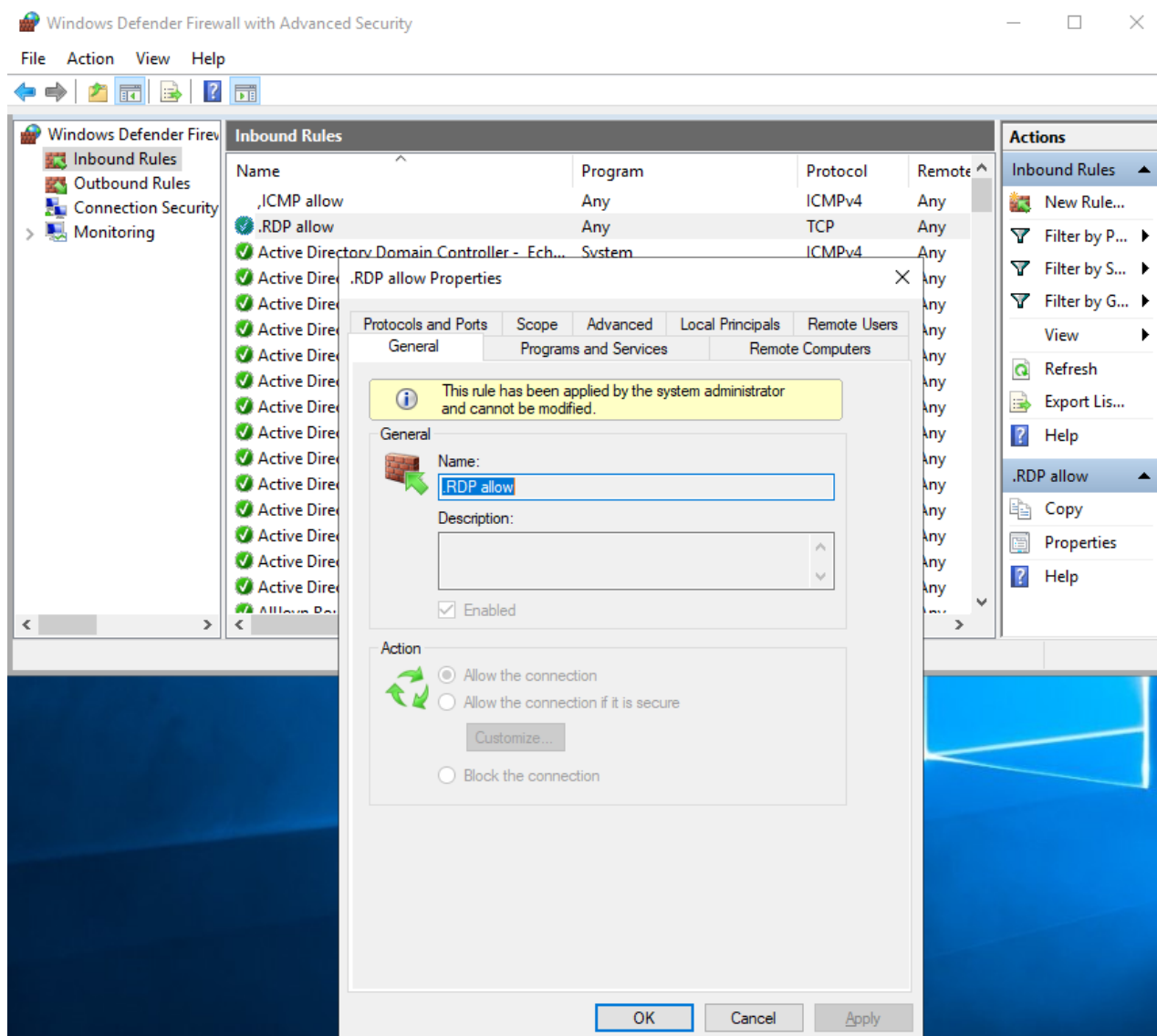
В отличие от локальной оснастки в GPO список правил изначально пуст, но сам процесс создания правил абсолютно такой же. Для создания нового правила надо кликнуть правой клавишей на нужном разделе и выбрать **New Rule**, после чего запустится уже знакомый мастер.



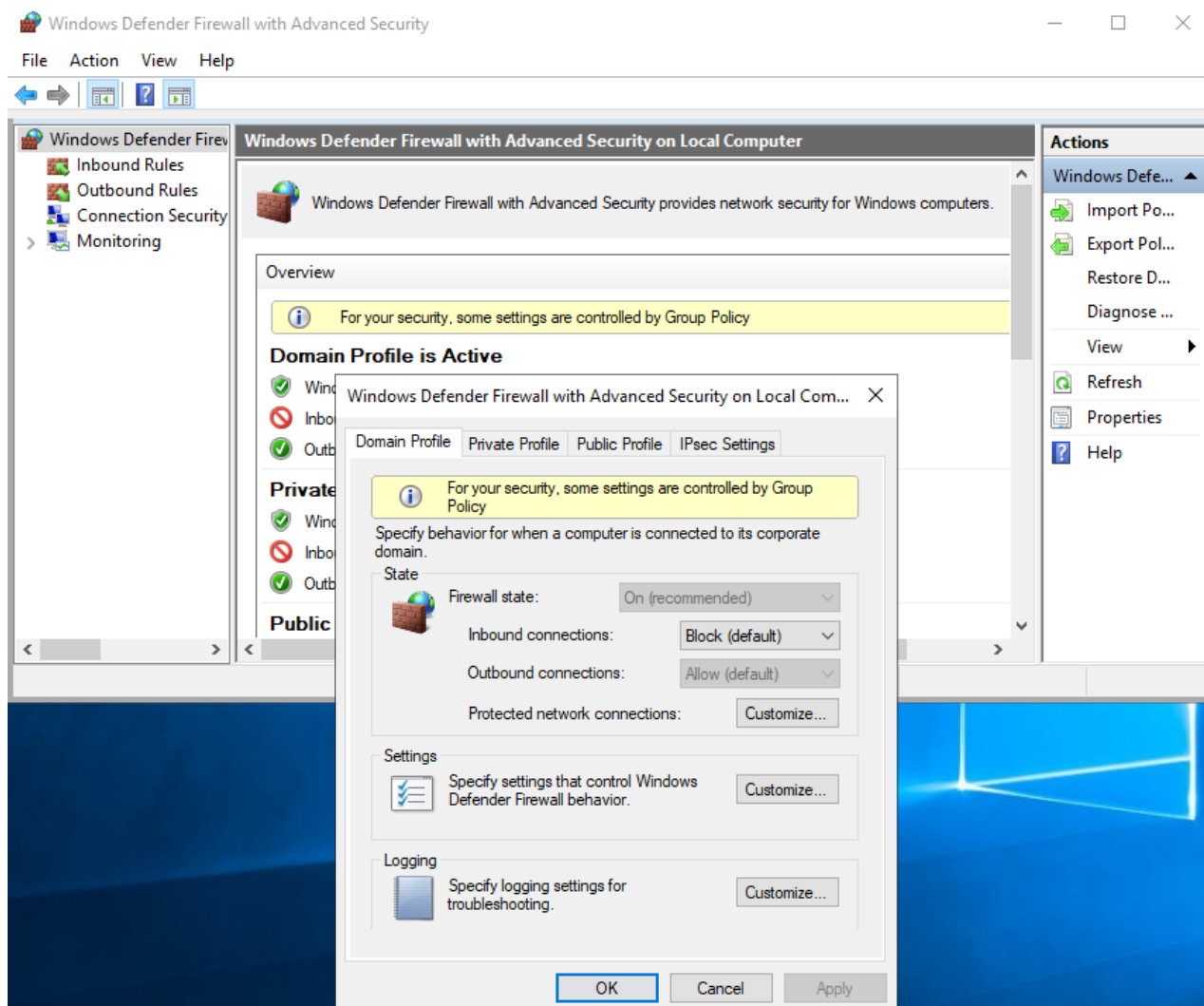
И созданные правила так же можно открывать и изменять.



А вот в локальной оснастке изменить или отключить правила, назначенные групповыми политиками, не получится.



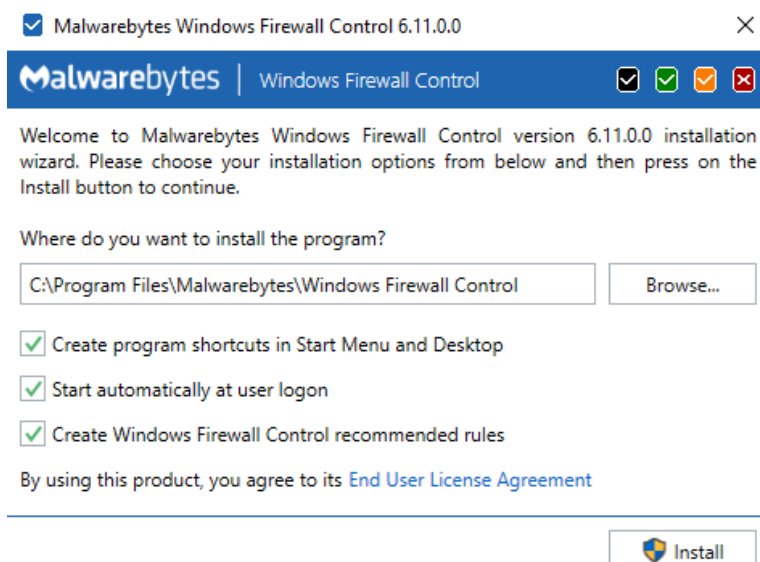
Как и глобальные настройки фаервола. Те параметры, которые назначены с помощью GPO, в локальной оснастке становятся недоступными для изменения.



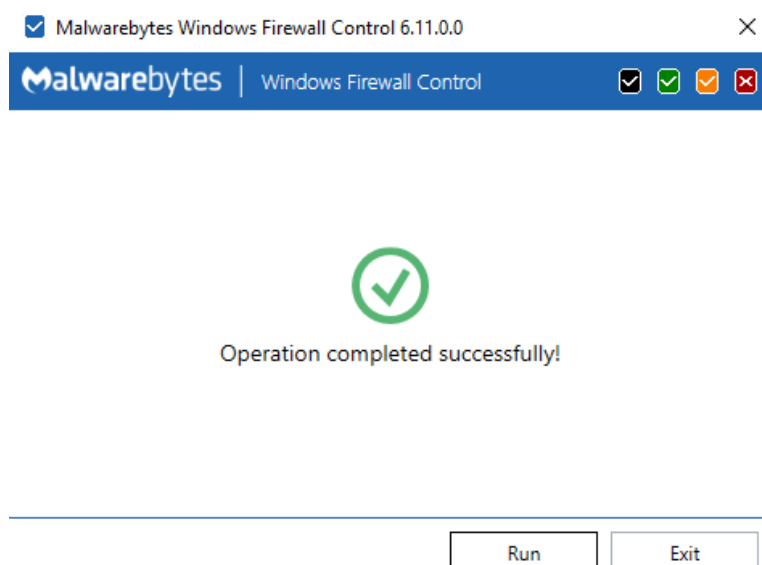
Windows Firewall Control

Windows Firewall Control — это оснастка для управления фаерволом Windows от стороннего разработчика Malwarebytes. Распространяется бесплатно, регулярно обновляется и поддерживается. Для скачивания не требуется даже регистрации.

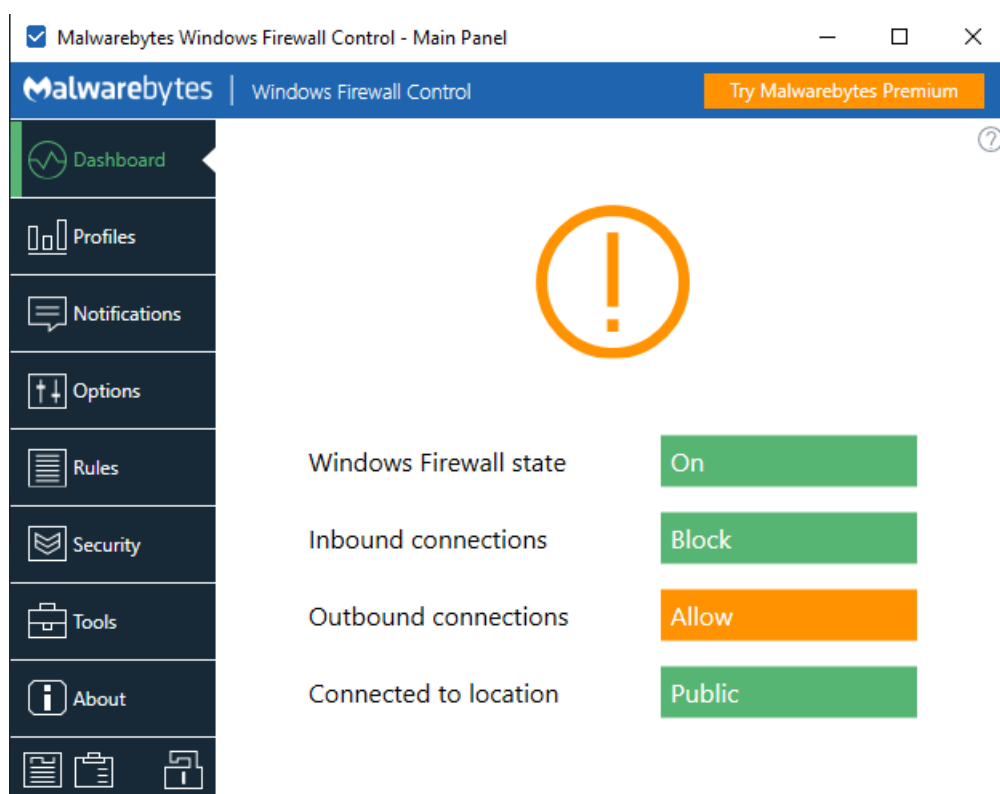
Установка простейшая — запускаем инсталлятор и ждем Install.



После установки можно сразу нажать Run, программа запустится и свернется в трей.



В главном окне программы мы видим состояние фаервола, действия по умолчанию и активный профиль сети. Что интересно, разрешенный по умолчанию исходящий трафик подсвечивается красным.

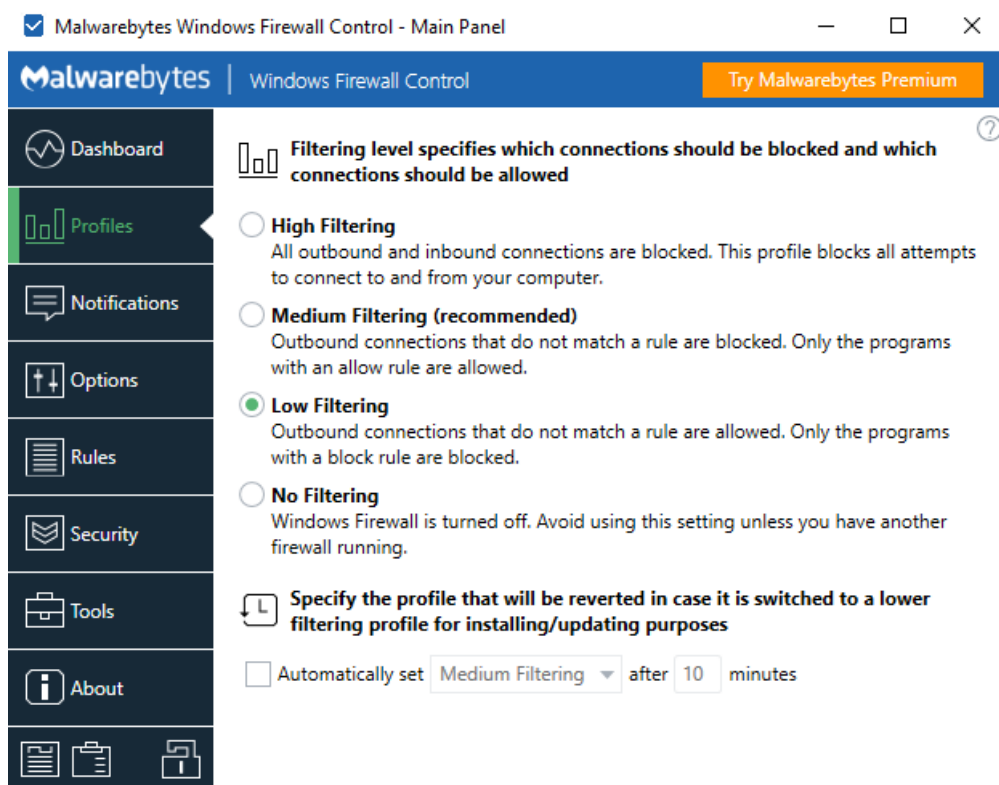


В Windows Firewall Control используется несколько другой подход к фильтрации трафика, отличный от стандартного. Мы можем выбрать один из 4 профилей, которые определяют политику доступа:

- **High Filtering** — запрещены все подключения, как входящие так и исходящие. Этот режим может потребоваться в том случае, если надо полностью изолировать сервер;

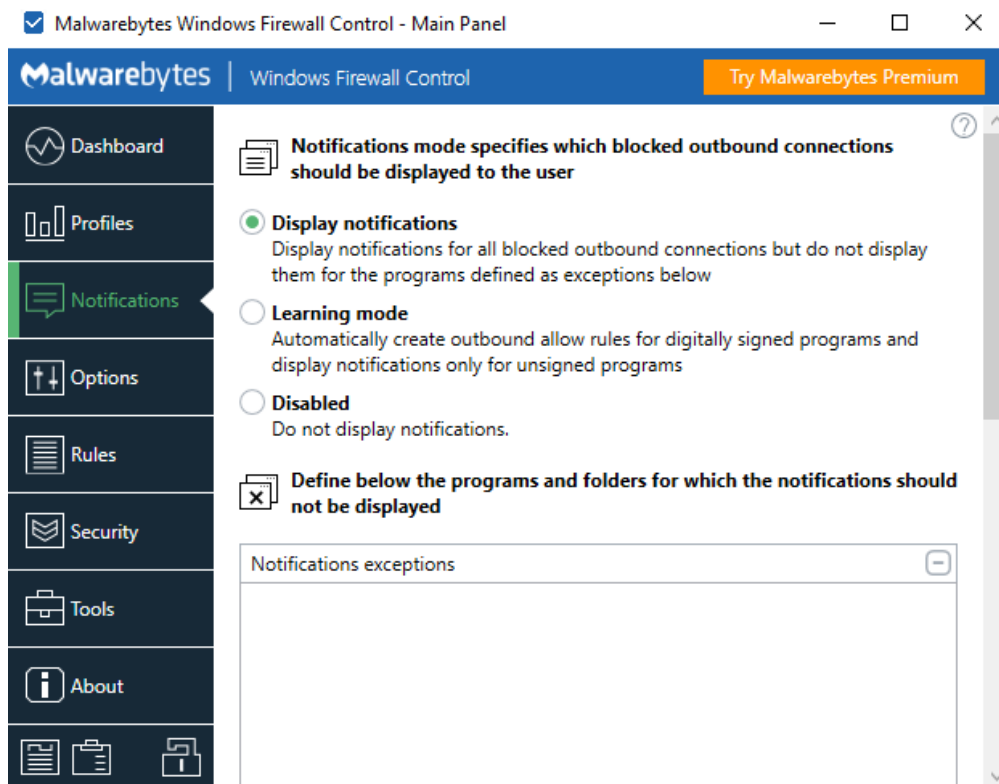
- **Medium Filtering** — входящие и исходящие подключения проверяются на соответствие правилам, не подпадающие под правила подключения блокируются;
- **Low Filtering** — на соответствие правилам проверяется только входящий трафик, исходящие подключения, не подходящие под действие правил, разрешаются;
- **No Filtering** — брандмауэр выключен. Этот режим может использоваться в том случае, если на компьютере установлен другой фаервол.

Как видите, по умолчанию предлагается использовать режим Medium, т.е. фильтровать исходящий трафик.



Но что произойдет в том случае, когда обнаружится попытка исходящего подключения, не предусмотренная ни в одном из имеющихся правил? Это решается настройкой уведомлений в разделе Notifications. Есть три варианта получения уведомлений:

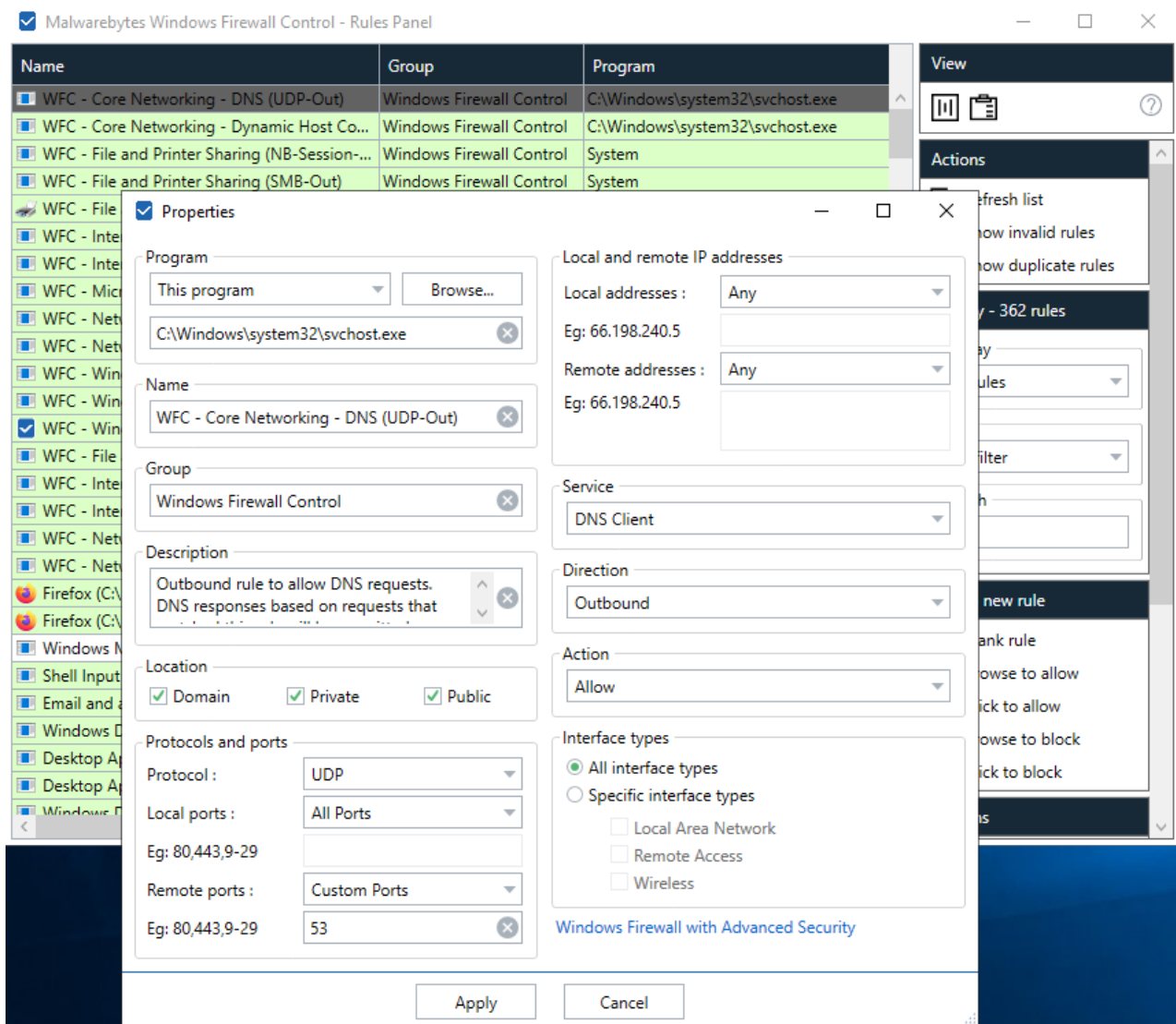
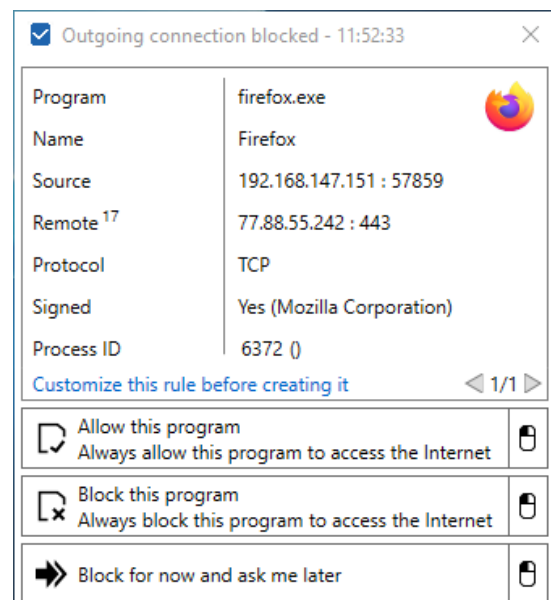
- **Display notifications** — показывать уведомления. Выбрав этот вариант можно получать уведомления всякий раз, когда новая программа пытается получить доступ наружу;
- **Learning mode** — режим обучения. В этом режиме автоматически создаются разрешающие правила для приложений, имеющих цифровую подпись, а для тех у кого ее нет выводится уведомление, как в первом случае;
- **Disabled** — уведомления отключены. В этом случае, если нет явно разрешающего правила, все подключения будут блокироваться без каких либо уведомлений.



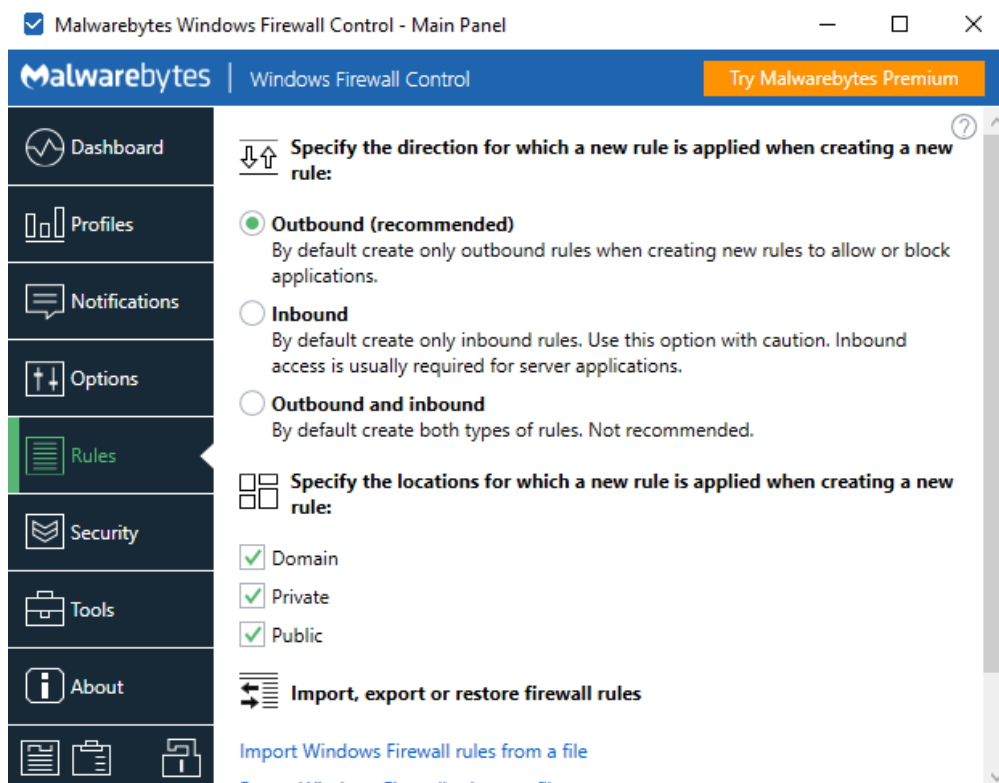
Если выбрать показ уведомлений, то при каждой попытке подключения будет выводиться окно с информацией — имя программы и ее исполняемый файл, наличие цифровой подписи, удаленный IP-адрес, к которому осуществляется подключение, используемый протокол и порт. Можно разрешить или запретить подключение для приложения на постоянной основе, либо заблокировать только текущее подключение. А щелкнув по значку приложения в правом верхнем углу, можно отправить исполняемый файл на антивирусную проверку в VirusTotal.

Если нажать **Allow the program**, то будет создано стандартное правило для приложения, где разрешены все исходящие подключения, на всех протоколах и портах. Если необходимо ограничить подключение, то можно выбрать **Customize this rule before creating** и настроить параметры правила вручную.

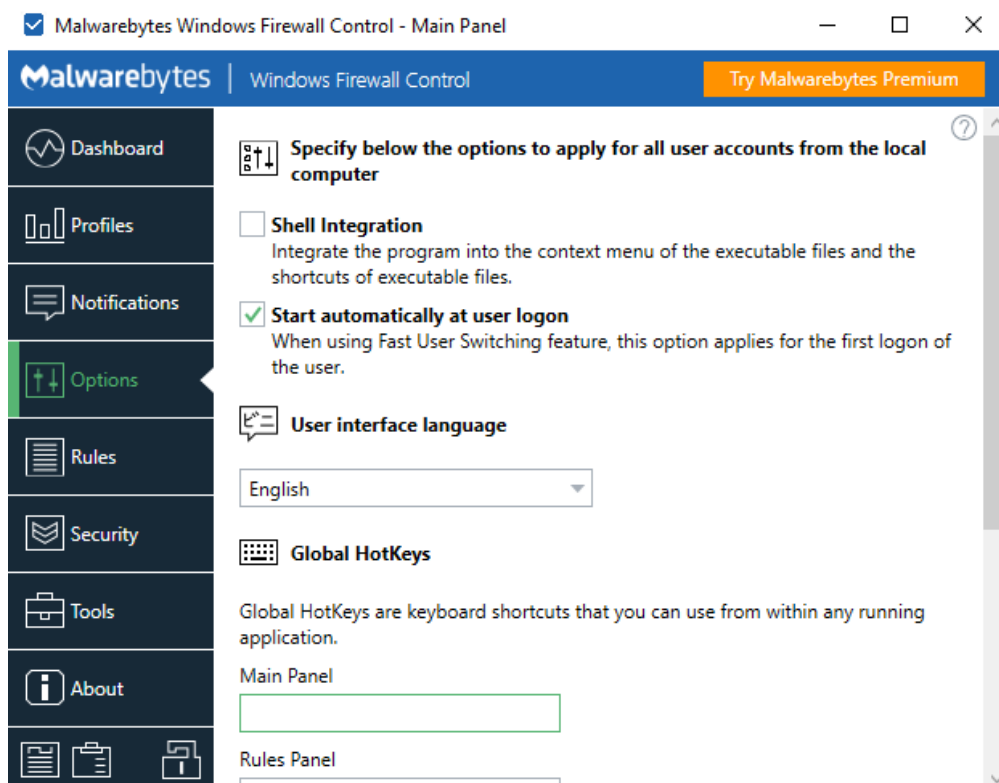
Панель со списком правил можно открыть, кликнув на значок в нижнем левом углу. Внешний вид панели отличается от привычной оснастки управления, но разобраться можно. Сами настройки правил сгруппированы более компактно, все в одном окне. Довольно удобно, хотя и непривычно.



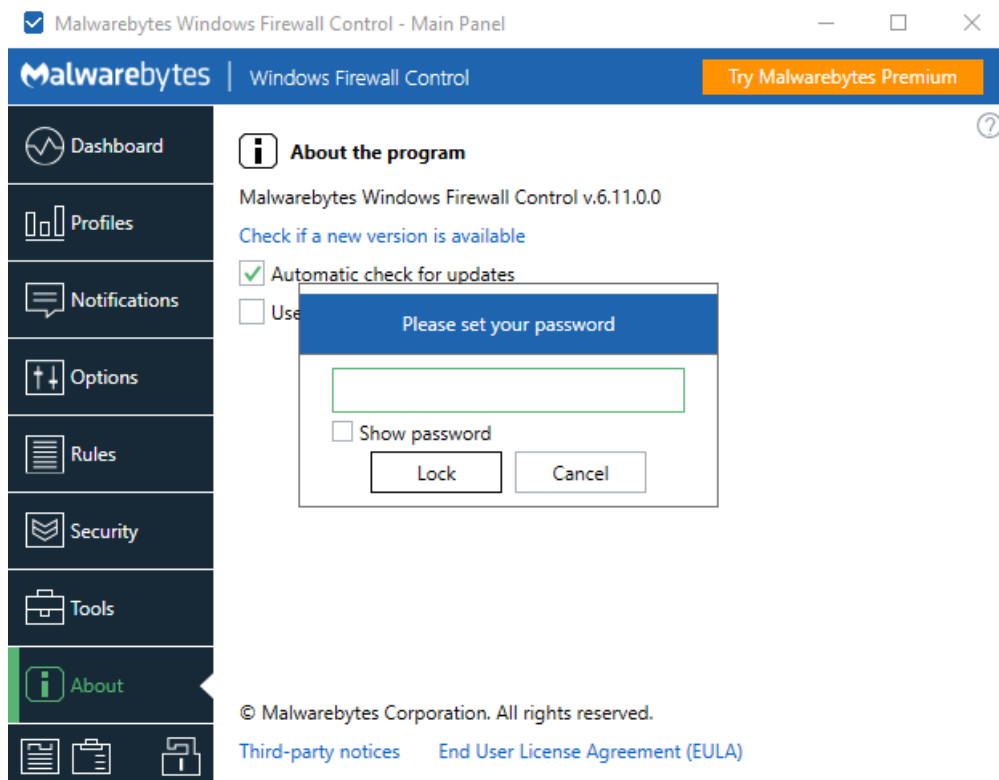
Базовые параметры для создаваемых по умолчанию правил можно настроить на вкладке Rules. Здесь же можно экспортировать текущую конфигурацию или импортировать правила из файла.



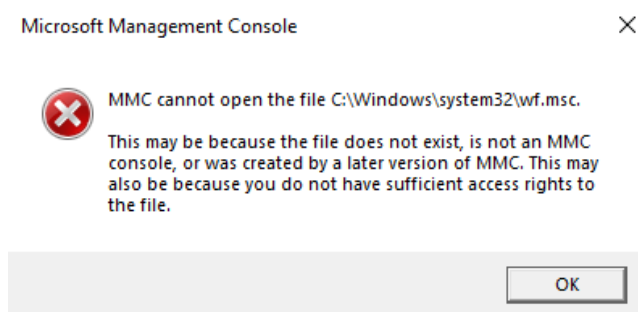
А параметры самого Windows Firewall Control настраиваются на вкладке Options. Здесь можно включить автоматический запуск приложения, встроить его в контекстное меню проводника, назначить сочетание клавиш для запуска панелей и изменить язык интерфейса. Кстати, русский язык в списке присутствует.



Еще из интересного — есть возможность заблокировать доступ к правилам, поставив пароль на вход.

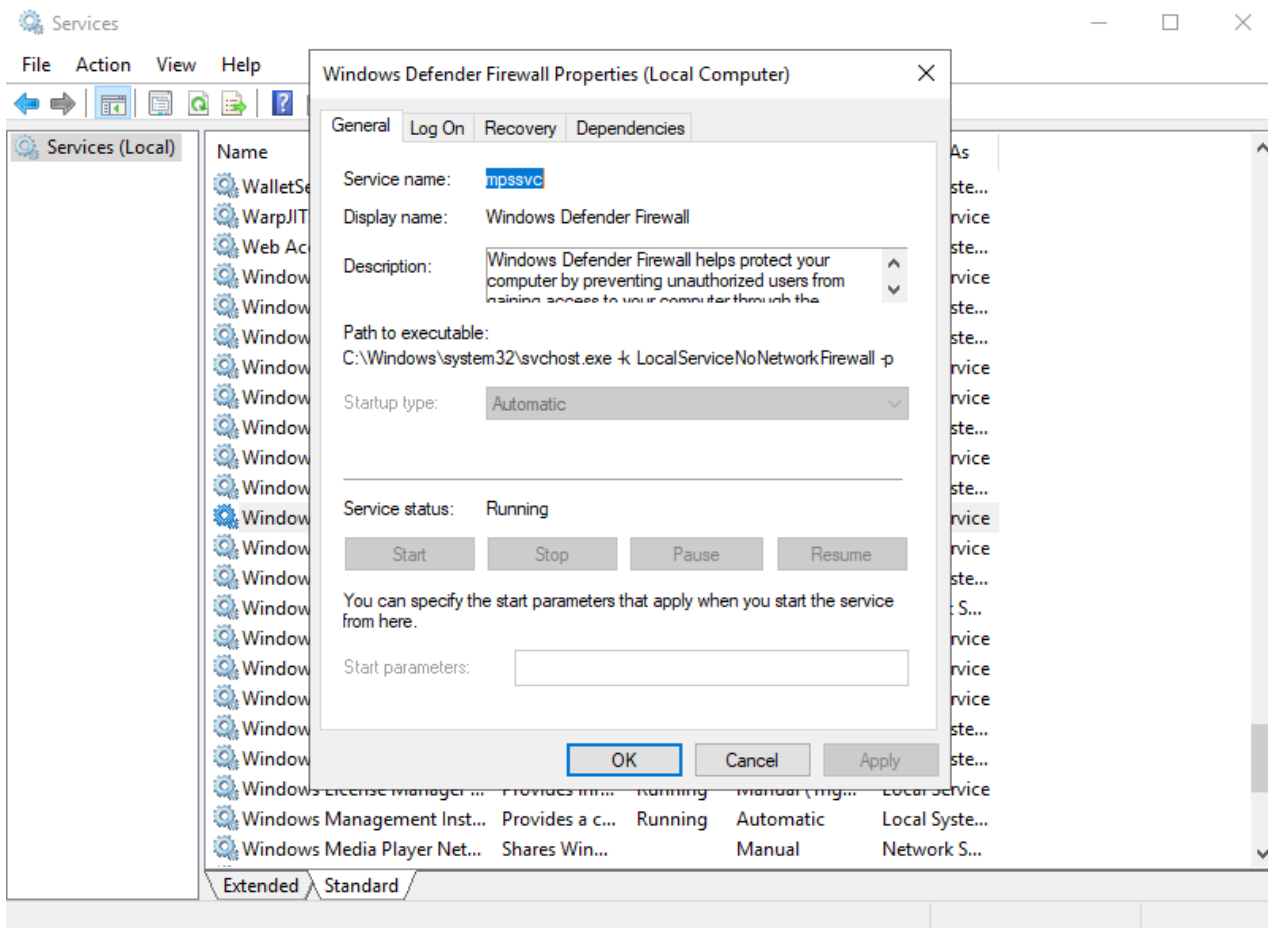


При этом перестает открываться и стандартная панель управления.

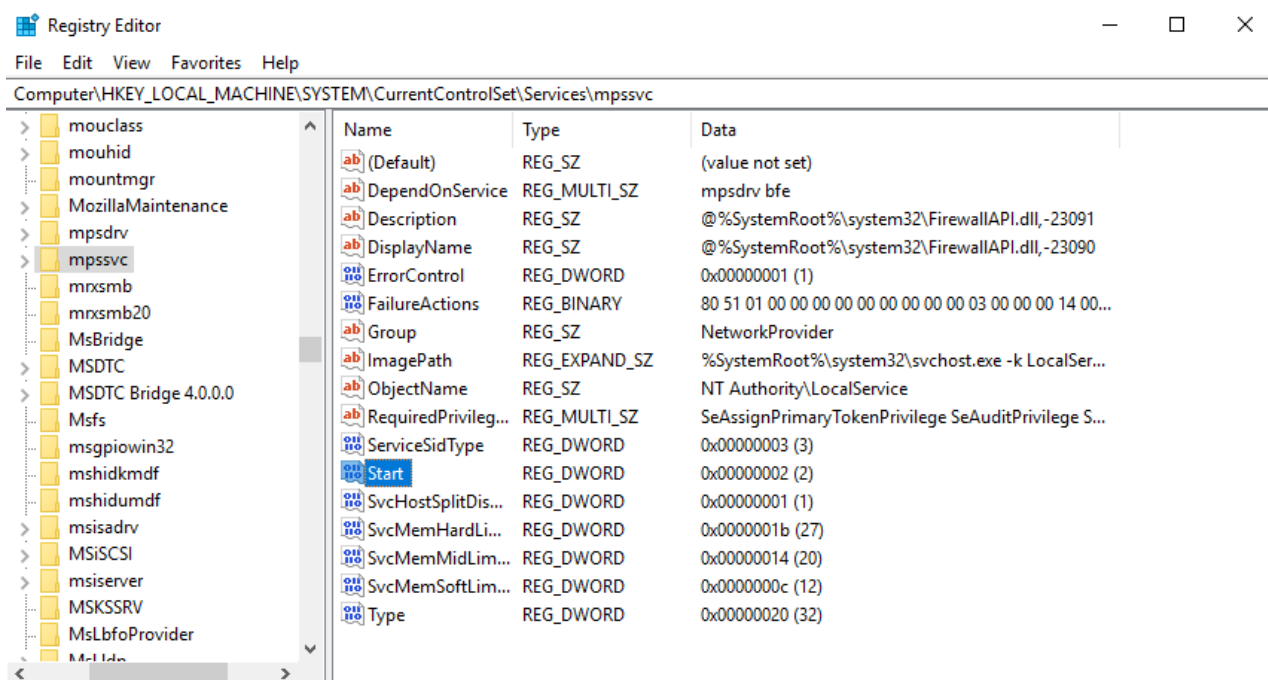


Принудительное отключение фаервола

Можно ли полностью выключить фаервол, погасив его службу? Если вы попытаете это сделать, то увидите, что все кнопки неактивны, выключить его или изменить режим запуска стандартными средствами невозможно. Но...

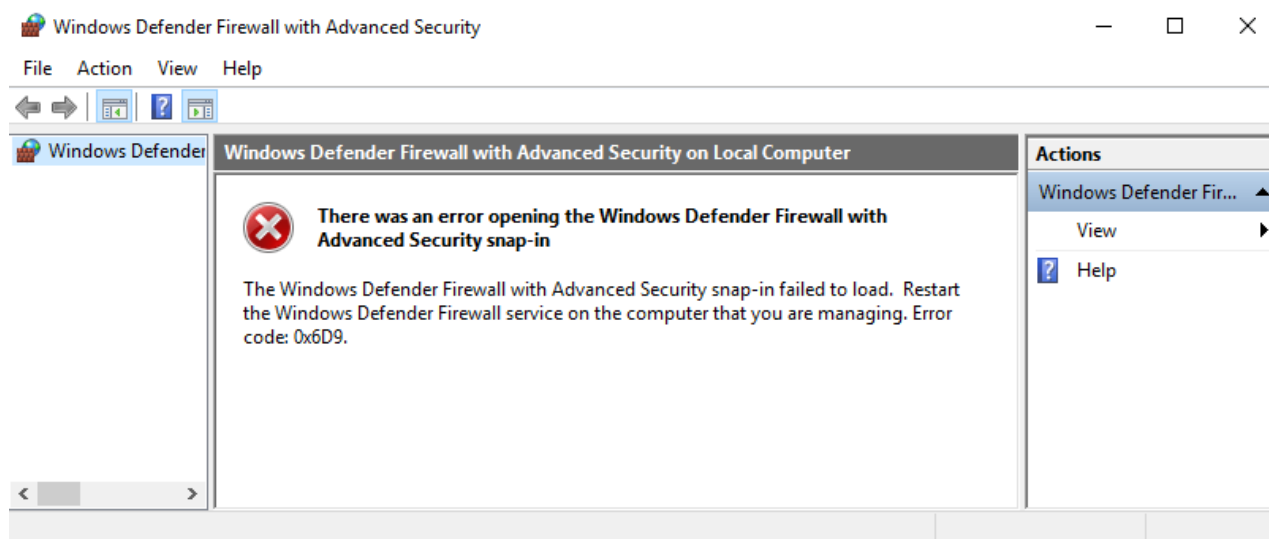
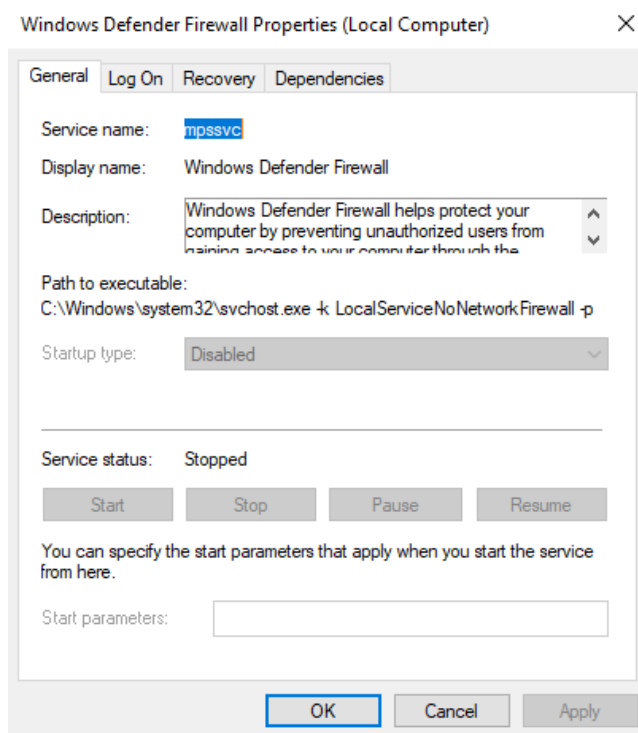


Настройки системных служб хранятся в реестре. В частности настройки фаервола можно найти в разделе HKLM\SYSTEM\CurrentControlSet\Services\mpssvc. За режим запуска отвечает параметр Start, и если изменить его значение на 4 и рестартовать компьютер



то фаервол не стартует, а останется в отключенном состоянии.

В этом случае станет недоступна и оснастка управления, включить его обратно можно только таким же способом, через реестр.



Заключение

В заключение скажу, что на данный момент встроенный фаервол Windows представляет из себя довольно мощное и эффективное средство защиты, хотя и специфическое. Из плюсов можно отметить то, что он есть в любой операционной системе Windows и включен по умолчанию. Он довольно гибко настраивается, при желании к нему можно прикрутить аутентификацию, шифрование и еще много всего.

Но основной его проблемой как была, так и осталась фильтрация исходящего трафика. По умолчанию исходящий трафик не фильтруется, и любой зловерд, проникнувший в систему, сможет беспрепятственно выходить в сеть. Если же включить фильтрацию исходящего трафика, то для большинства клиентских

приложений потребуются явно разрешать подключения, в противном случае они не смогут нормально функционировать. А с учетом всех нюансов настройки это довольно большой объем работ.

Стоит ли заморачиваться с тонкой настройкой или оставить все по умолчанию — решайте сами. Но, в любом случае, наличие включенного фаервола лучше, чем его отсутствие.