Настройка правил брандмауэра Windows Defender с помощью групповых политик

Брандмауэр Microsoft Defender Firewall встроен во все современные версии Windows и Windows Server и позволяет настраивать правила фильтрации входящего и/или исходящего сетевого трафика на компьютере. Правила Windows Firewall можно настраивать локально на компьютере пользователя (с помощью консоли `wf.msc`, команды `netsh` или встроенного PowerShell модуля NetSecurity). На компьютерах Windows, которые добавлены в домен Active Directory вы можете централизованно управлять правилами и настройками Microsoft Defender Firewall с помощью групповых политик.

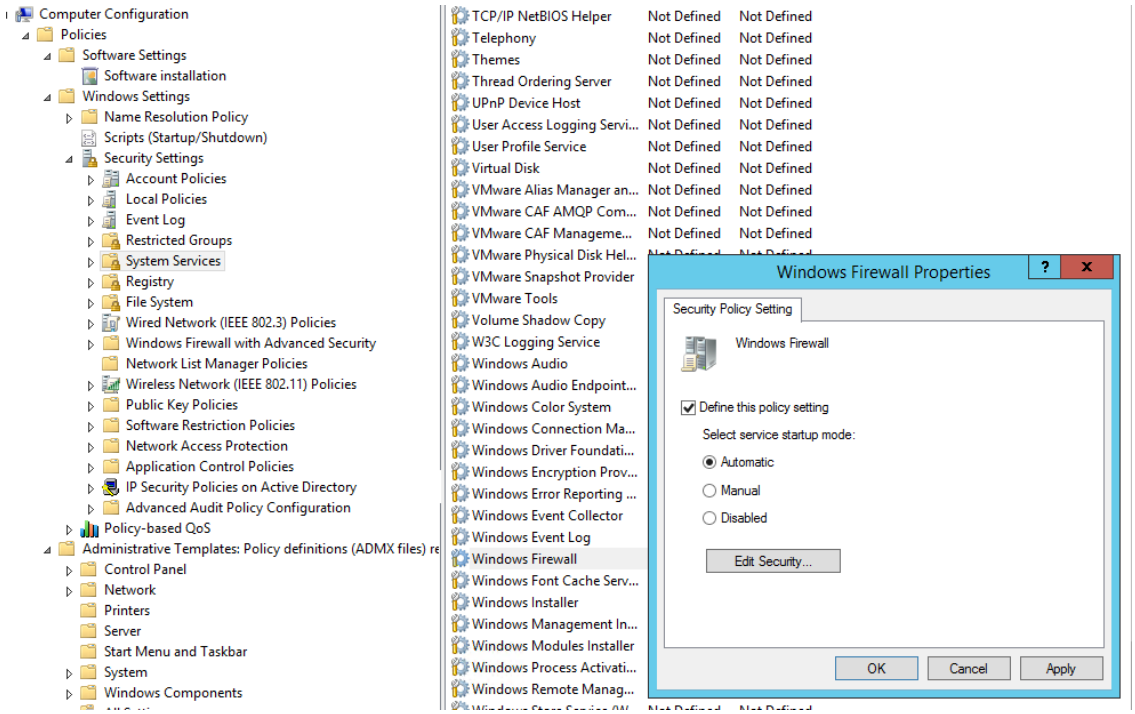
В крупных организациях правила фильтрации портов обычно выносятся на уровень маршрутизаторов, L3 коммутаторов или выделенных межсетевых экранах. Однако ничего не мешает вам распространить ваши правила ограничения сетевого доступа Windows Firewall к рабочим станциям или серверам Windows.

Содержание:

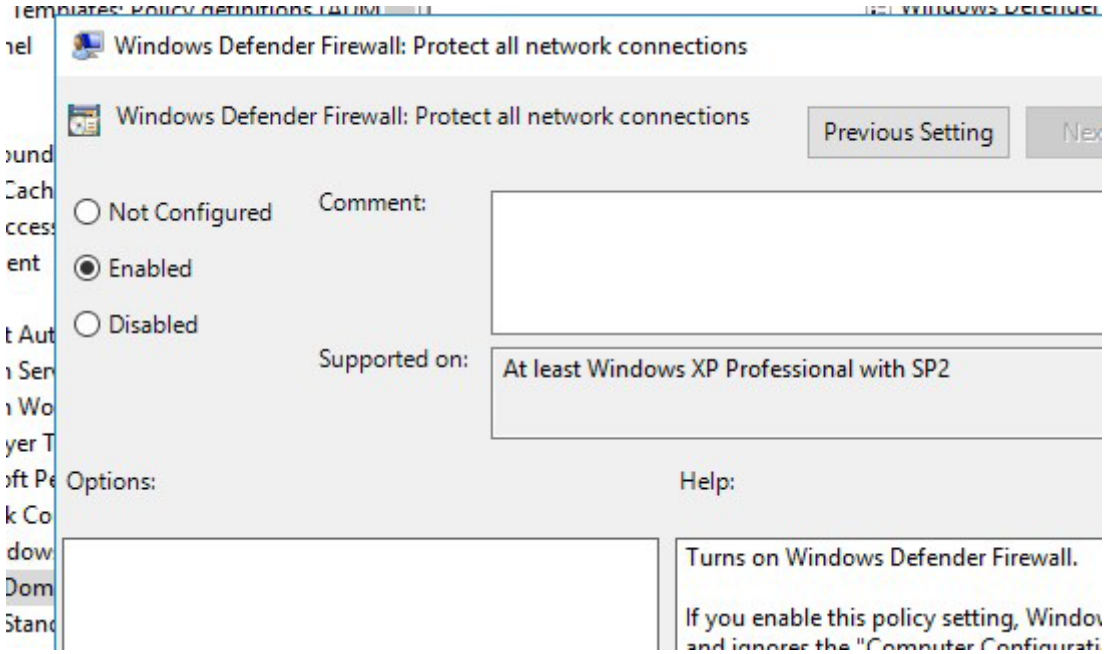
Включить Windows Defender с помощью GPO

Запустите консоль управления доменными групповыми политиками (Group Policy Management Console, `gpmc.msc`), создайте новую GPO с именем **gpoFirewallDefault** и перейдите в режим редактирования (Edit).

Чтобы пользователи (даже с правами локального админа) не могли выключить службу брандмауэра, желательно настроить автоматический запуск службы Windows Firewall через GPO. Для этого перейдите в раздел **Computer Configuration -> Windows Settings -> Security Settings -> System Services**. Найдите в списке служб **Windows Firewall** и измените тип запуск службы на автоматический (Define this policy setting -> Service startup mode Automatic). Убедитесь, что у пользователей нет прав на остановку служб.

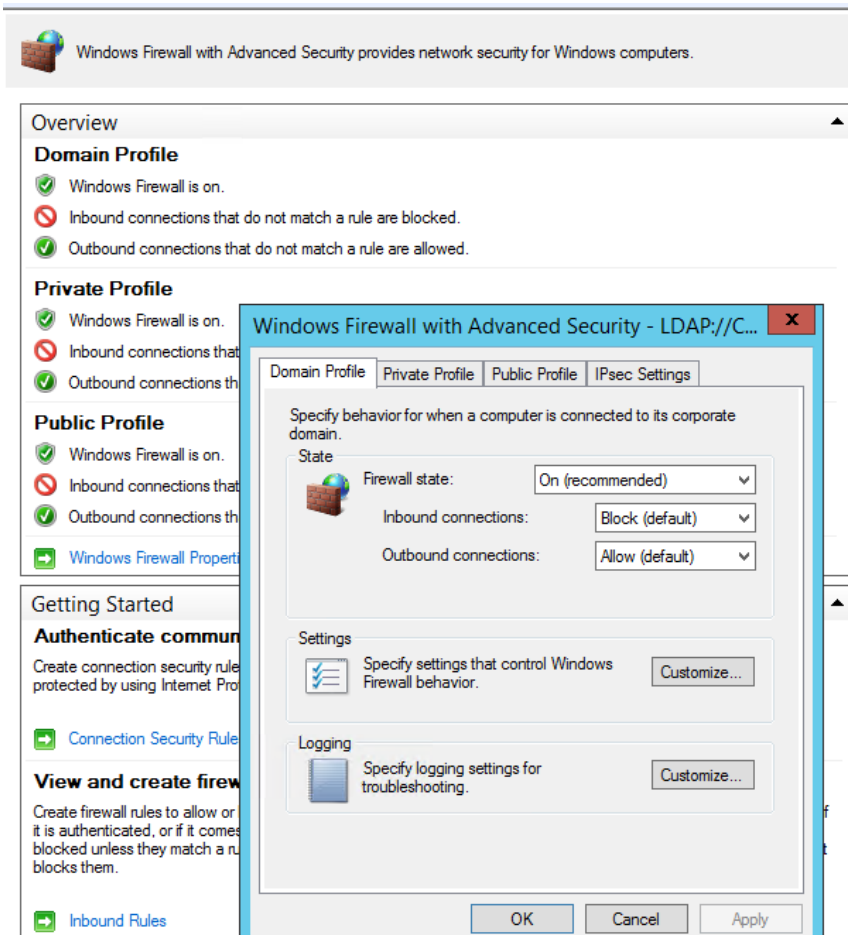


Затем перейдите в раздел **Computer Configuration -> Policies -> Administrative Templates -> Network -> Network Connections -> Windows Defender -> Firewall -> Domain Profile** и включите политику **Windows Defender Firewall: Protect all network connections**.

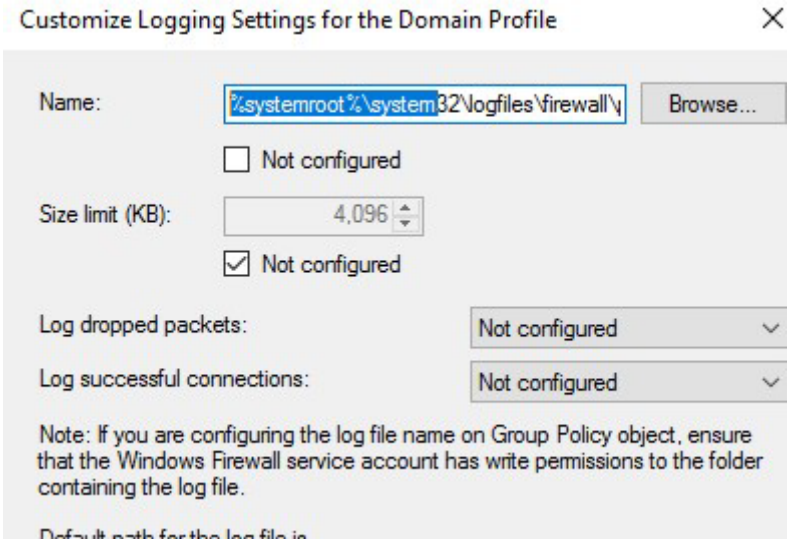


Откройте свойства **Windows Firewall with Advanced Security** в разделе GPO **Computer Configuration -> Windows Settings -> Security Settings**.

На всех трех вкладках Domain Profile, Private Profile и Public Profile (что такое профиль сети в Windows) измените состояние Firewall state на **On (recommended).** В зависимости от политик безопасности в вашей организации вы можете указать, что все входящие подключения по умолчанию запрещены (Inbound connections -> Block), а исходящие разрешены (Outbound connections -> Allow). Сохраните изменения.



В целях отладки правил файервола вы можете включить запись логов Windows Defender в текстовый файл %systemroot%\system32\logfiles\firewall\pfirewall.log (по умолчанию). Можно включить логирование отклоненных пакетов (Log dropped packets) или пакетов, который были разрешены правилами файервола (Log successfully connections). По-умолчанию логирование сетевых соединений в Windows отключено.



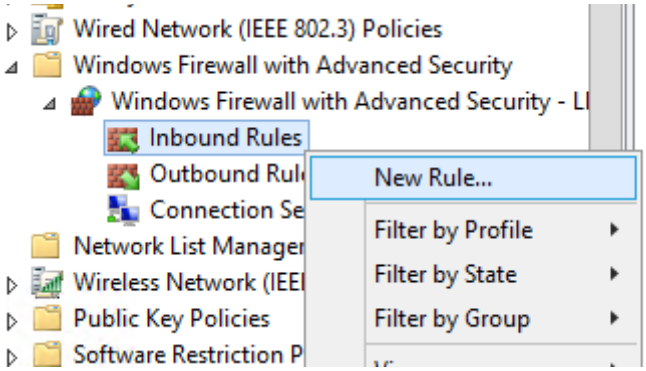
Создать правила файервола Windows с помощью групповой политики

Теперь рассмотрим, как создать правила файервола Microsoft Defender с помощью GPO. Для настройки правил, перейдите в раздел **Computer Configuration -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security.**

Интерфейс этого раздела напоминает локальную консоль управления брандмауэром Windows и состоит из трех секций:

- Inbound rules
- Outbound rules
- Connection security rules

Попробуем создать разрешающее входящее правило файервола. Например, мы хотим разрешить подключение к компьютерам по RDP (порт по умолчанию TCP 3389). Щелкните ПКМ по разделу Inbound Rules и выберите пункт меню New Rule. Запустится мастер создания нового правила брандмауэра.

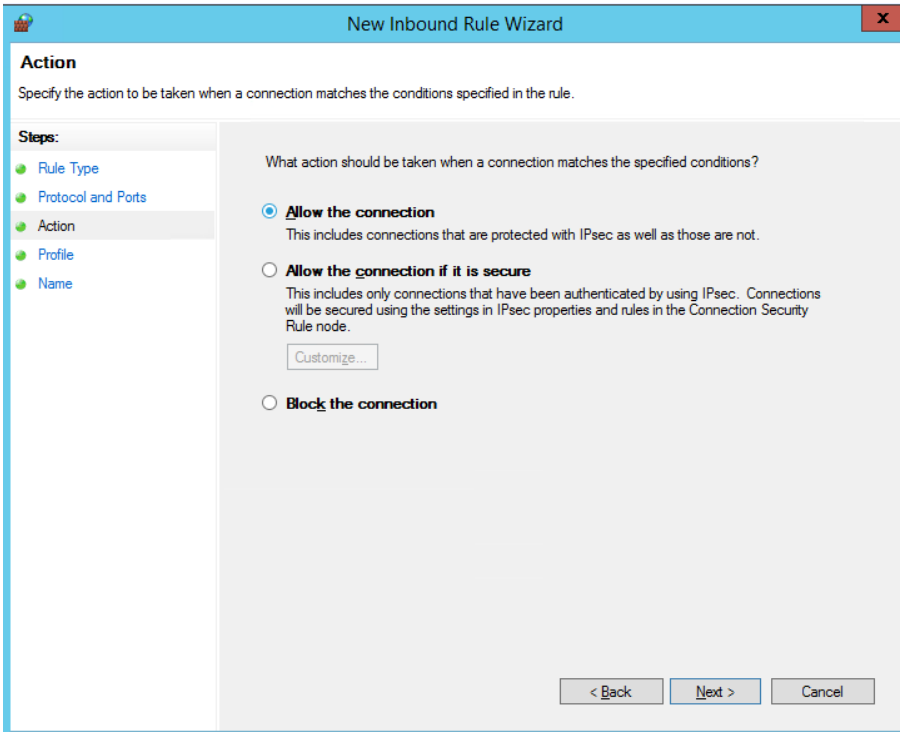


Выберите тип правила. Можно разрешить доступ для:

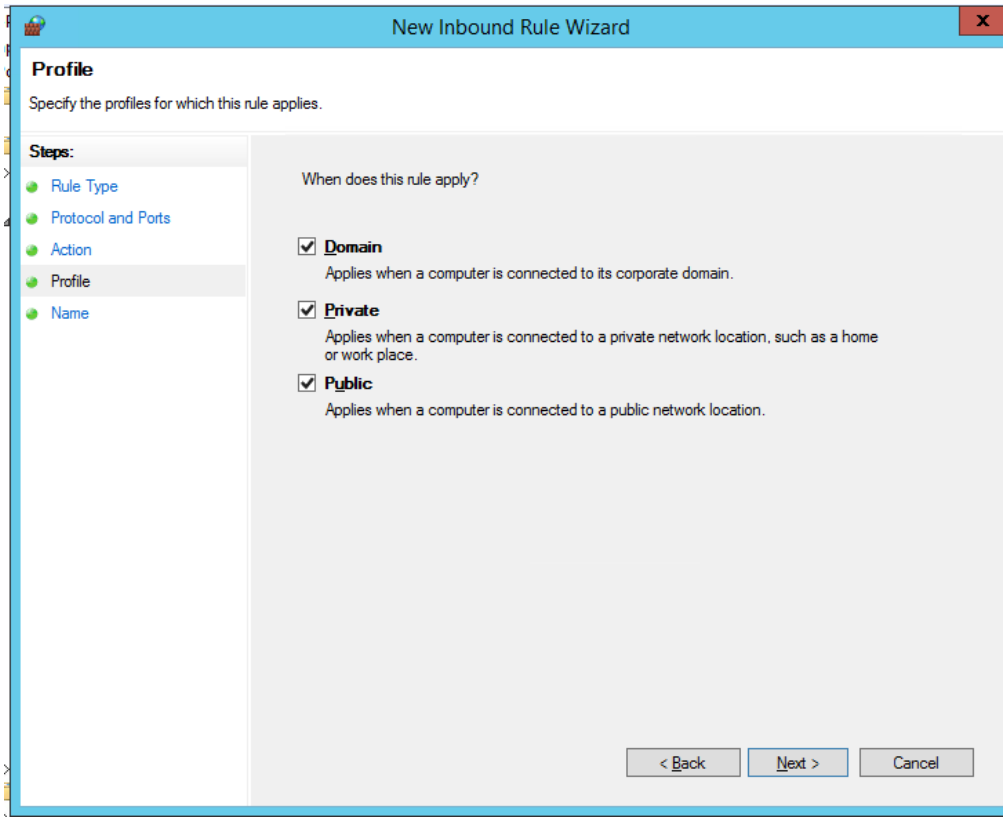
- Программы (Program) – можно выбрать исполняемый exe программы;
- Порта (Port) – выбрать TCP/UDP порт или диапазон портов;
- Преднастроенное правило (Predefined) – выбрать одно из стандартных правил Windows, в которых уже имеются правила доступа (описаны как исполняемые файлы,

так и порты) к типовым службам (например, AD, Http, DFS, BranchCache, удаленная перезагрузка, SNMP, KMS, WinRM и т.д.);

- Собственное правило (Custom) – здесь можно указать программу, протокол (другие протоколы помимо TCP и UDP, например, ICMP, GRE, L2TP, IGMP и т.д.), IP адреса клиентов или целые IP подсети.
- Далее нужно выбрать что нужно сделать с таким сетевым подключением: разрешить (Allow the connection), разрешить если оно безопасное или заблокировать (Block the connection).



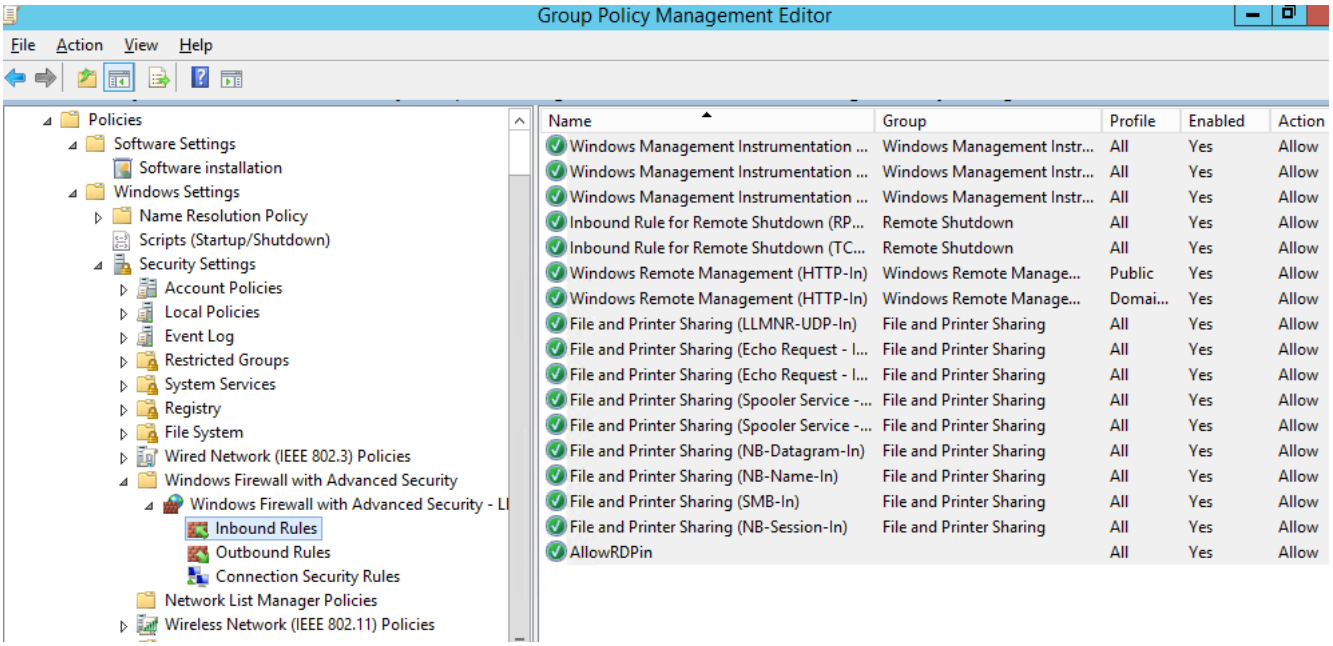
Осталось выбрать профили сети, для которых нужно применить это правило. Можно оставить все профили (Domain, Private и Public).



На последнем шаге нужно указать имя правило и его описание. Нажмите кнопку Finish и оно появится в списке правил брандмауэра.

В современных версиях Windows для трафика удаленного рабочего стола RDP также используется порт UDP 3389. Поэтому создайте второе правила Microsoft Defender и для этого порта.

Аналогичным образом вы можете настроить другие правила для входящего трафика, которые должны применятся к вашим клиентам Windows.



Вы можете создать правила как для входящего и исходящего трафика.

Выше мы рассмотрели, как использовать графический мастер для создания правил Windows Defender Firewall. Также вы можете сформировать список правил в простом текстовой форме и быстро создать правила для групповой политики Defender.

Перейдите в раздел Computer Configuration -> Policies -> Administrative Templates -> Network -> Network Connections -> Windows Defender Profile -> Domain Profile и откройте параметр **Windows Defender Firewall: Define inbound port exceptions**. Здесь вы можете создать список правил с помощью простых текстовых строчек.

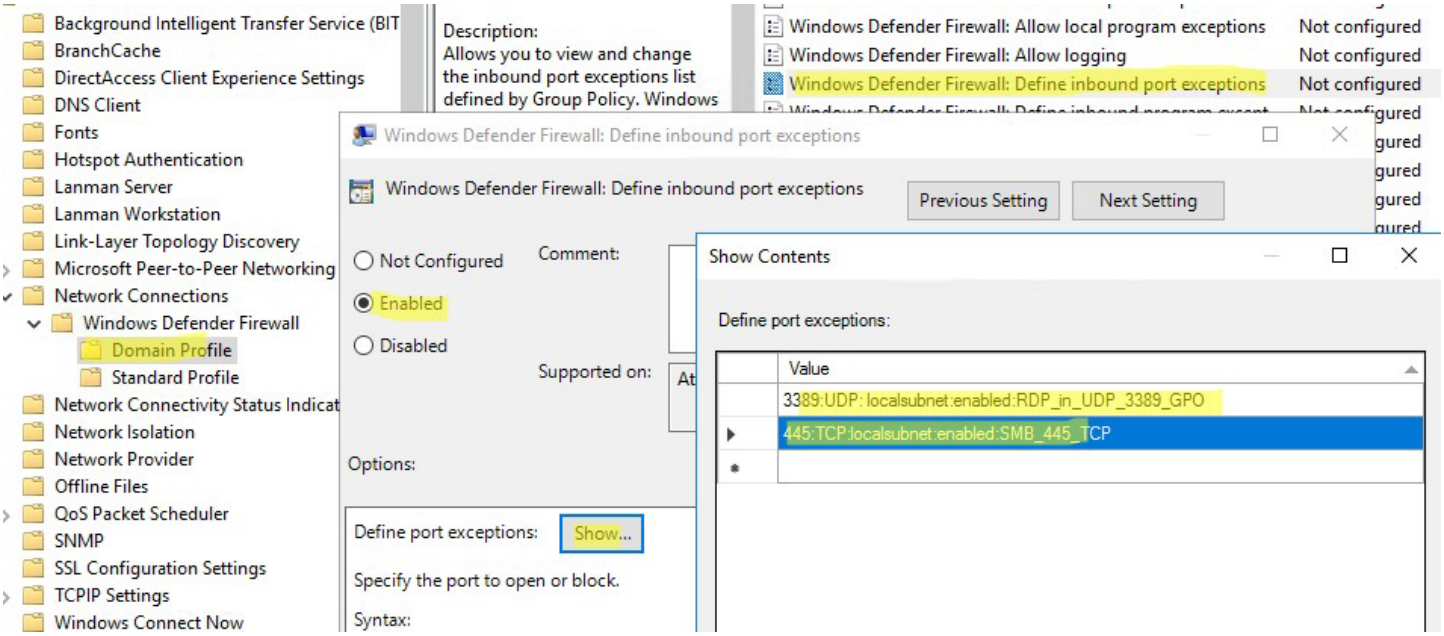
Ниже представлен список правил, который я хочу добавить в групповую политику

```
3389:UDP:localsubnet:enabled:RDP_in_UDP_3389_GPO

445:TCP:localsubnet:enabled:SMB_445_TCP

443:TCP:192.168.100.10:enabled:HTTP_in_445_TCP
```

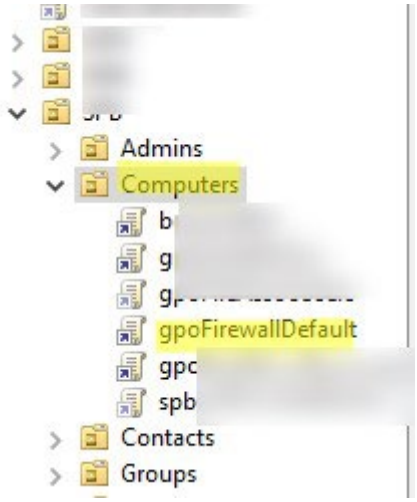
Нажмите кнопку **Show** и построчно скопируйте ваши правила в окно **Define port exceptions**.



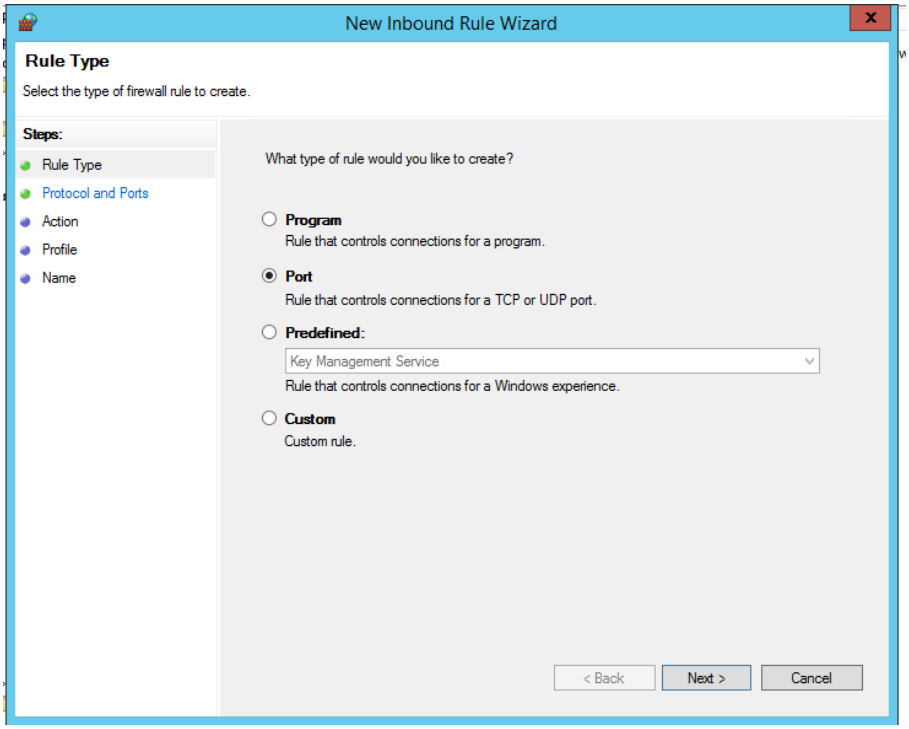
Этот способ позволяет вам быстро создать большое количество входящих правил для файервола Windows.

Применить политики брандмауэра Microsoft Defender к компьютерам Windows

Теперь осталось назначить политику Firewall-Policy на OU (Organizational Unit) с компьютерами пользователей. Найдите в консоли Group Policy Management нужный OU, щелкните по нему правой кнопкой и выберите **Link an Existing GPO**. Выберите в списке вашу политику.

- 

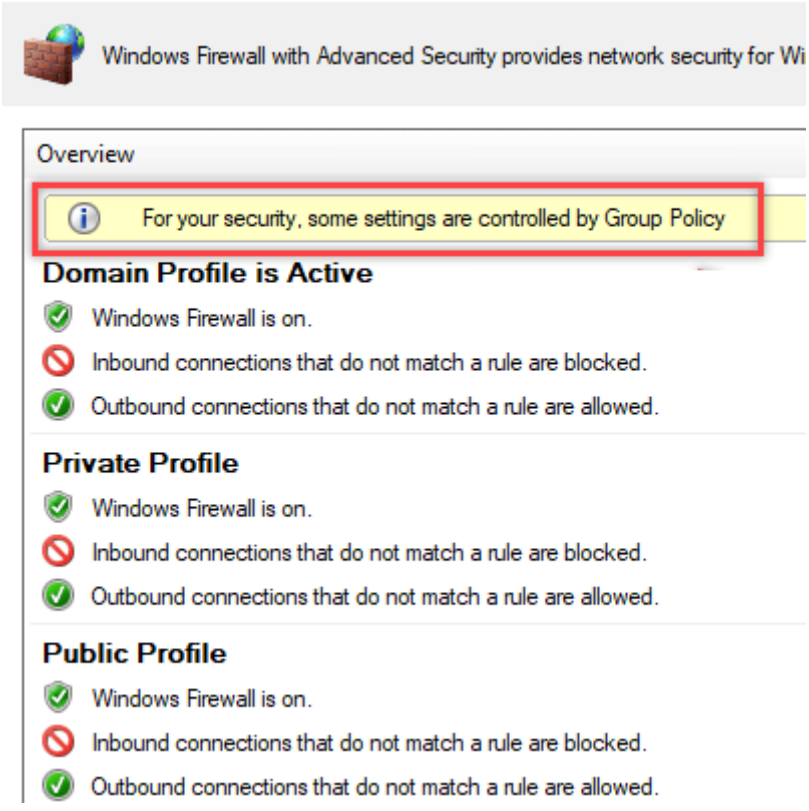
- Важно. Прежде, чем применять политику файервола к OU с продуктивными компьютерами, настоятельно рекомендуется проверить ее на тестовых компьютерах. Из-за некорректной настройки брандмауэра вы можете полностью заблокировать сетевой доступ компьютерам. Для диагностики применения групповых политик используйте утилиту gpresult.exe.



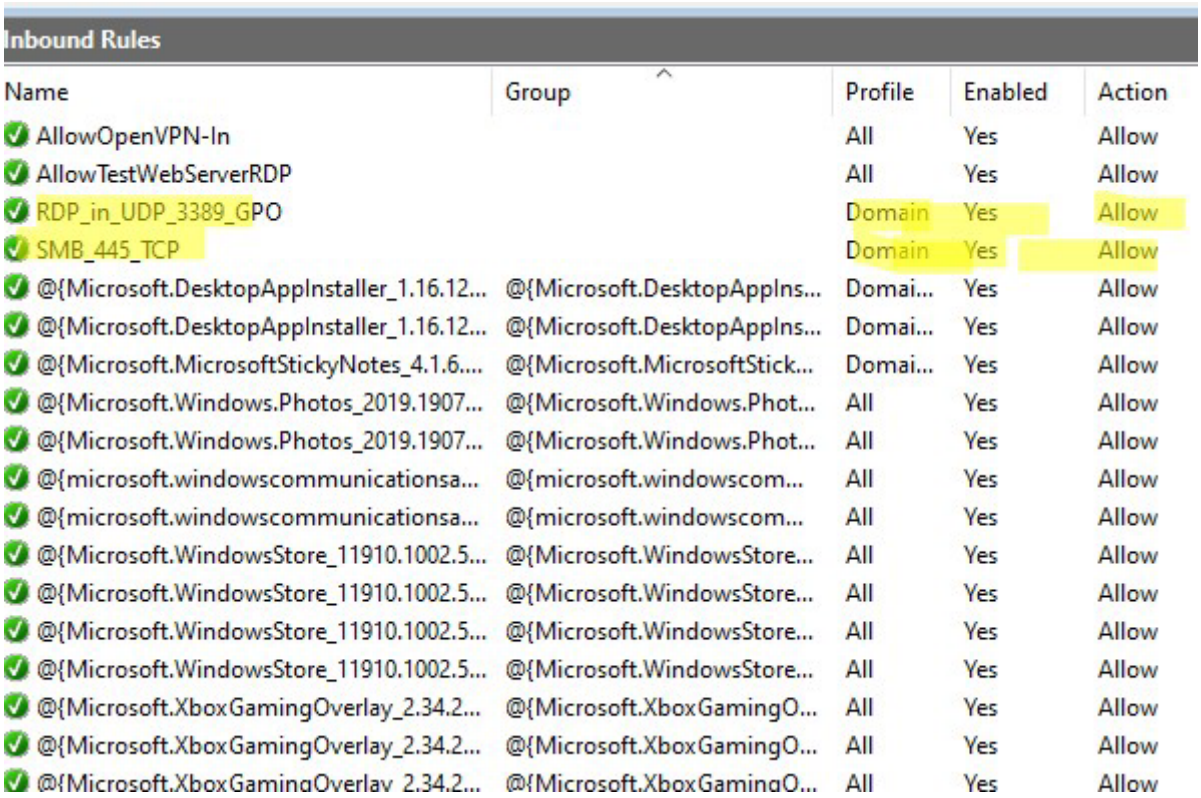
В нашем случае мы выберем правило **Port**. В качестве протокола укажем **TCP**, в качестве порта – Specific local ports -> **3389**.

Обновите настройки групповых политик на клиентах (`gpupdate /force`). Проверьте, что указанные вами порты открыты на компьютерах пользователей (можно использовать командлет Test-NetConnection или утилиту Portqry).

На компьютере пользователя откройте Панель управления\Система и безопасность\Брандмауэр Защитника Windows и убедитесь, что появилась надпись: *Для обеспечения безопасности, некоторые параметры управляются групповой политикой* (For your security, some settings are controlled by Group Policy), и используются заданные вами настройки брандмаэера.



Пользователь теперь не может изменить настройки брандмауэра, а в списке Inbound Rules должны быть указаны все созданные вами правила. Обратите внимание, что по умолчанию новые правила из GPO добавляются к уже существующим локальным правилам файервола.



Inbound Rules

Name	Group	Profile	Enabled	Action
AllowOpenVPN-In		All	Yes	Allow
AllowTestWebServerRDP		All	Yes	Allow
RDP_in_UDP_3389_GPO		Domain	Yes	Allow
SMB_445_TCP		Domain	Yes	Allow
@{Microsoft.DesktopAppInstaller_1.16.12...	@{Microsoft.DesktopAppIns...	Domai...	Yes	Allow
@{Microsoft.DesktopAppInstaller_1.16.12...	@{Microsoft.DesktopAppIns...	Domai...	Yes	Allow
@{Microsoft.MicrosoftStickyNotes_4.1.6....	@{Microsoft.MicrosoftStick...	Domai...	Yes	Allow
@{Microsoft.Windows.Photos_2019.1907...	@{Microsoft.Windows.Phot...	All	Yes	Allow
@{Microsoft.Windows.Photos_2019.1907...	@{Microsoft.Windows.Phot...	All	Yes	Allow
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allow
@{microsoft.windowscommunicationsa...	@{microsoft.windowscom...	All	Yes	Allow
@{Microsoft.WindowsStore_11910.1002.5...	@{Microsoft.WindowsStore...	All	Yes	Allow
@{Microsoft.WindowsStore_11910.1002.5...	@{Microsoft.WindowsStore...	All	Yes	Allow
@{Microsoft.WindowsStore_11910.1002.5...	@{Microsoft.WindowsStore...	All	Yes	Allow
@{Microsoft.WindowsStore_11910.1002.5...	@{Microsoft.WindowsStore...	All	Yes	Allow
@{Microsoft.XboxGamingOverlay_2.34.2...	@{Microsoft.XboxGamingO...	All	Yes	Allow
@{Microsoft.XboxGamingOverlay_2.34.2...	@{Microsoft.XboxGamingO...	All	Yes	Allow
@{Microsoft.XboxGamingOverlay_2.34.2...	@{Microsoft.XboxGamingO...	All	Yes	Allow

Также вы можете вывести текущие настройки Windows Defender с помощью команды:

```
netsh firewall show state
```

Или можно представить список правил в табличной форме с помощью скрипта PowerShell:

```
Get-NetFirewallRule -Action Allow -Enabled True -Direction Inbound |
Format-Table -Property Name,
@{Name='Protocol';Expression={($PSItem | Get-NetFirewallPortFilter).Protocol}},
@{Name='LocalPort';Expression={($PSItem | Get-NetFirewallPortFilter).LocalPort}},
@{Name='RemotePort';Expression={($PSItem | Get-
NetFirewallPortFilter).RemotePort}},
@{Name='RemoteAddress';Expression={($PSItem | Get-
NetFirewallAddressFilter).RemoteAddress}},
Enabled,Profile,Direction,Action
```

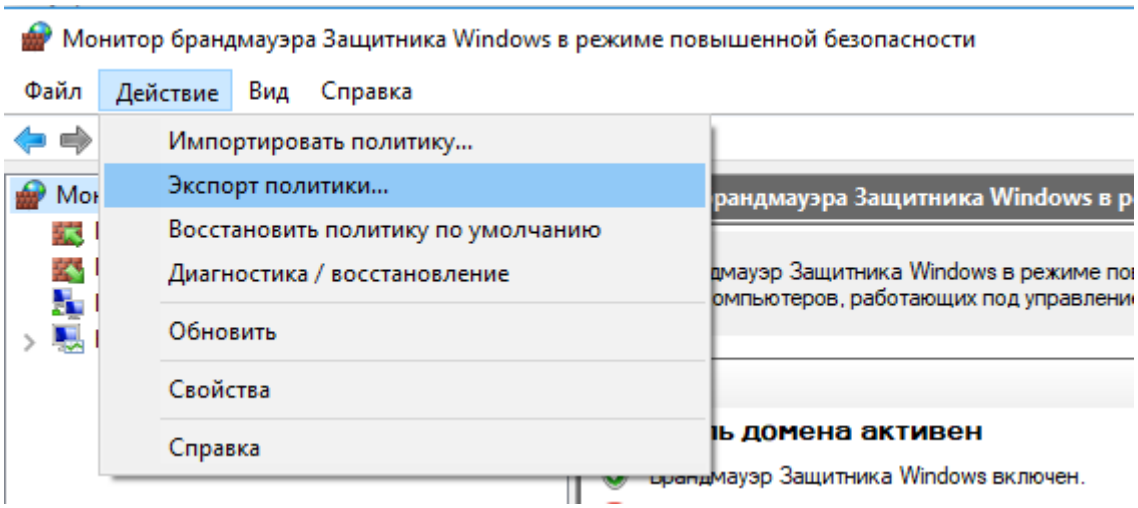
```
PS C:\WINDOWS\system32> Get-NetFirewallRule -Action Allow -Enabled True -Direction Inbound |
>> Format-Table -Property Name,
>> @{Name='Protocol';Expression={($PSItem | Get-NetFirewallPortFilter).Protocol}},
>> @{Name='LocalPort';Expression={($PSItem | Get-NetFirewallPortFilter).LocalPort}},
>> @{Name='RemotePort';Expression={($PSItem | Get-NetFirewallPortFilter).RemotePort}},
>> @{Name='RemoteAddress';Expression={($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Profile,Direction,Action

Name                          Protocol LocalPort RemotePort RemoteAddress Enabled Profile Direction Action
----                          -------- --------- ---------- ------------- ------- ------- --------- ------
WiFiDirect-KM-Driver-In-TCP   TCP      Any       Any        Any              True     Any   Inbound  Allow
WiFiDirect-KM-Driver-In-UDP   UDP      Any       Any        Any              True     Any   Inbound  Allow
DeliveryOptimization-TCP-In   TCP      7680      Any        Any              True     Any   Inbound  Allow
DeliveryOptimization-UDP-In   UDP      7680      Any        Any              True     Any   Inbound  Allow
CDPSvc-In-UDP                 UDP      Any       Any        Any              True ...vate   Inbound  Allow
CDPSvc-In-TCP                 TCP      Any       Any        Any              True ...vate   Inbound  Allow
CDPSvc-WFD-In-TCP             TCP      Any       Any        Any              True  Public   Inbound  Allow
CoreNet-ICMP6-DU-In           ICMPv6   RPC       Any        Any              True     Any   Inbound  Allow
CoreNet-ICMP6-PTB-In          ICMPv6   RPC       Any        Any              True     Any   Inbound  Allow
CoreNet-ICMP6-TE-In           ICMPv6   RPC       Any        Any              True     Any   Inbound  Allow
CoreNet-ICMP6-PP-In           ICMPv6   RPC       Any        Any              True     Any   Inbound  Allow
CoreNet-ICMP6-NDS-In          ICMPv6   RPC       Any        Any              True     Any   Inbound  Allow
```

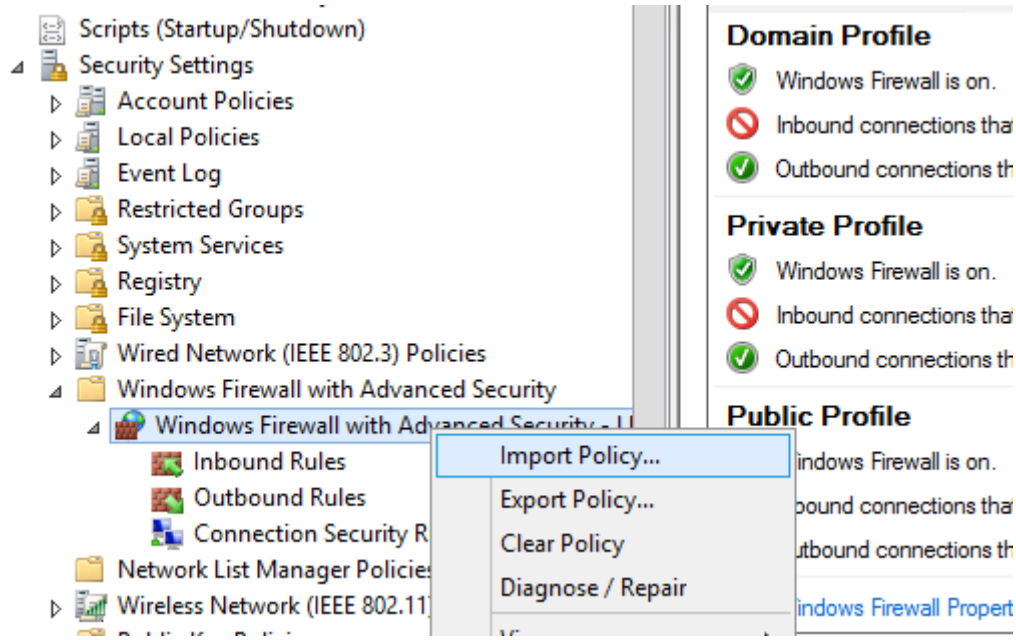
Импорт и экспорт правил брандмауэра Windows в GPO

Консоль Windows Defender Firewall позволяет экспортировать и импортировать текущие настройки файервола в текстовый файл. Вы можете настроить правила брандмауэра на эталонном компьютере и экспортировать их в консоль групповых политики.

Настройте нужные правила, замет встаньте на корень оснастки брандмауэра (Монитор Брандмауэра Защитника Windows в режиме повышенной безопасности) и выберите пункт Действие -> **Экспорт политики**



Политика выгружается в WFW файл, который можно импортировать в редакторе Group Policy Management Editor, выбрав пункт **Import Policy** и указав путь к файлу wfw (текущие настройки будут перезаписаны).



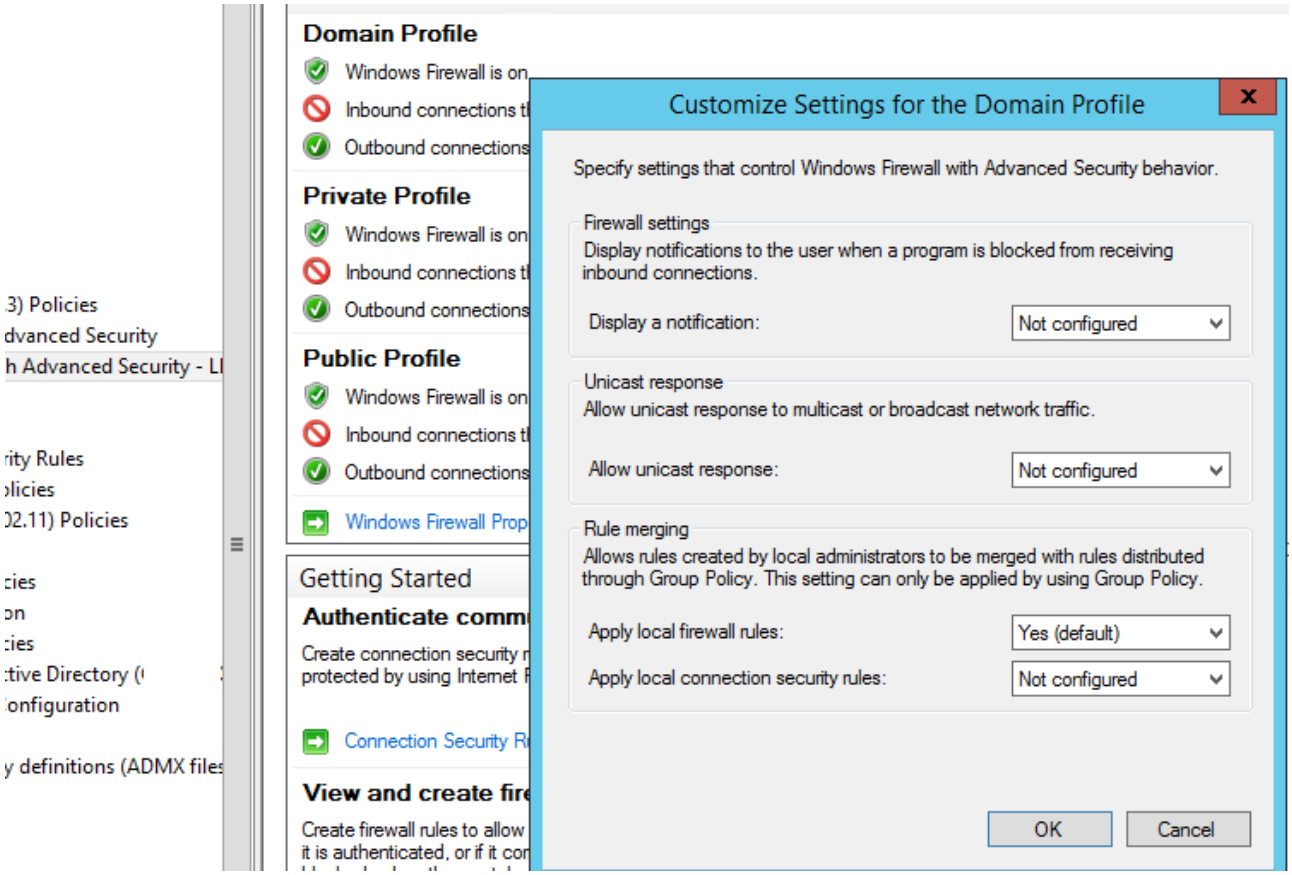
Доменные и локальные правила Microsoft Defender

В GPO вы можете настроить, хотите ли вы разрешить локальным администраторам создавать на своих компьютерах собственные правила брандмауэра и как эти правила должны объединяться с правилами, назначенными через GPO.

Откройте в GPO свойства политики (Windows Firewall Properties), выберите вкладку с профилем (Domain) и нажмите кнопку Customize.

Обратите внимание на настройки в разделе **Rule merging**. По умолчанию режим объединения правил включен. Вы можете принудительно указать, что локальный администратор может

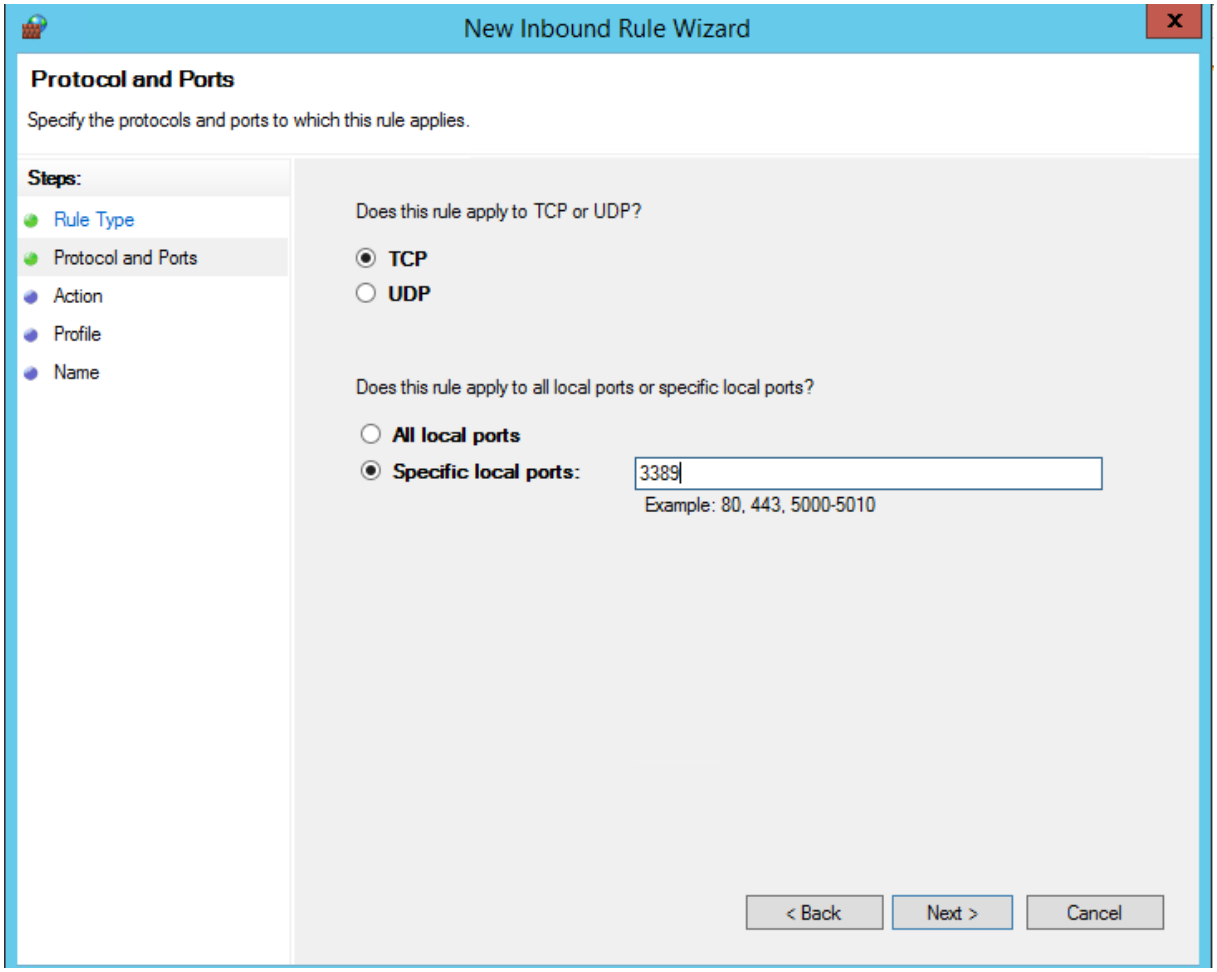
создавать собственные правила брандмауэра: в параметре **Apply local firewall rules** выберите **Yes (default)**.



Совет. Блокирующие правила файервола имеют приоритет над разрешающими. Т.е. пользователь не сможет создать собственное разрешающее правило доступа, противоречащее запрещающему правилу, настроенному администратором через GPO. Однако пользователь может создать локальное запрещающее правило, даже если этот доступ разрешен администратором в политике.

Несколько советов об управлении брандмауэром Windows через GPO

- Создавайте отдельные политики с правилами брандмауэра для серверов и рабочих станций (для каждой группы одинаковых серверов возможно придется создать собственные политики в зависимости от их роли). Т.е. правила файервола для контроллера домена, почтового Exchange сервера, сервера с ролью Remote Desktop Services Host (RDSH) или Microsoft SQL Server будут отличаться;
- Для более точного нацеливания политики на клиентов можно использовать WMI фильтры GPO (например, вы можете привязать политику к хостам определенной IP подсети)
- Какие порты нужно открыть для той или иной службы нужно искать в документации на сайте разработчика. Процесс довольно кропотливый и на первый взгляд сложный. Но постепенно вполне реальной прийти к работоспособной конфигурации Windows файервола, который разрешает только одобренные подключения и блокирует все остальное. По опыту хочу отметить, что на ПО Microsoft можно довольно быстро найти список используемых TCP/UDP портов.


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
3389
Example: 80, 443, 5000-5010
< Back
Next >
Cancel