

Как добавить правило в Windows Firewall

Файрвол (Firewall) - это устройство сетевой безопасности, которое отслеживает входящий и исходящий сетевой трафик. Файрвол разрешает или блокирует пакеты данных на основе набора правил безопасности. Часто можно встретить идентичный по смыслу термин Брандмауэр. Также в русском языке встречается написание "фаервол".

С помощью брандмауэра (Firewall) можно ограничить доступ в интернет для всех, кроме конкретных программ. Также можно разрешить соединяться с компьютером, на котором он установлен только из внешней сети или только из внутренней сети, только по определенному порту, с определенных ip-адресов и т.д.

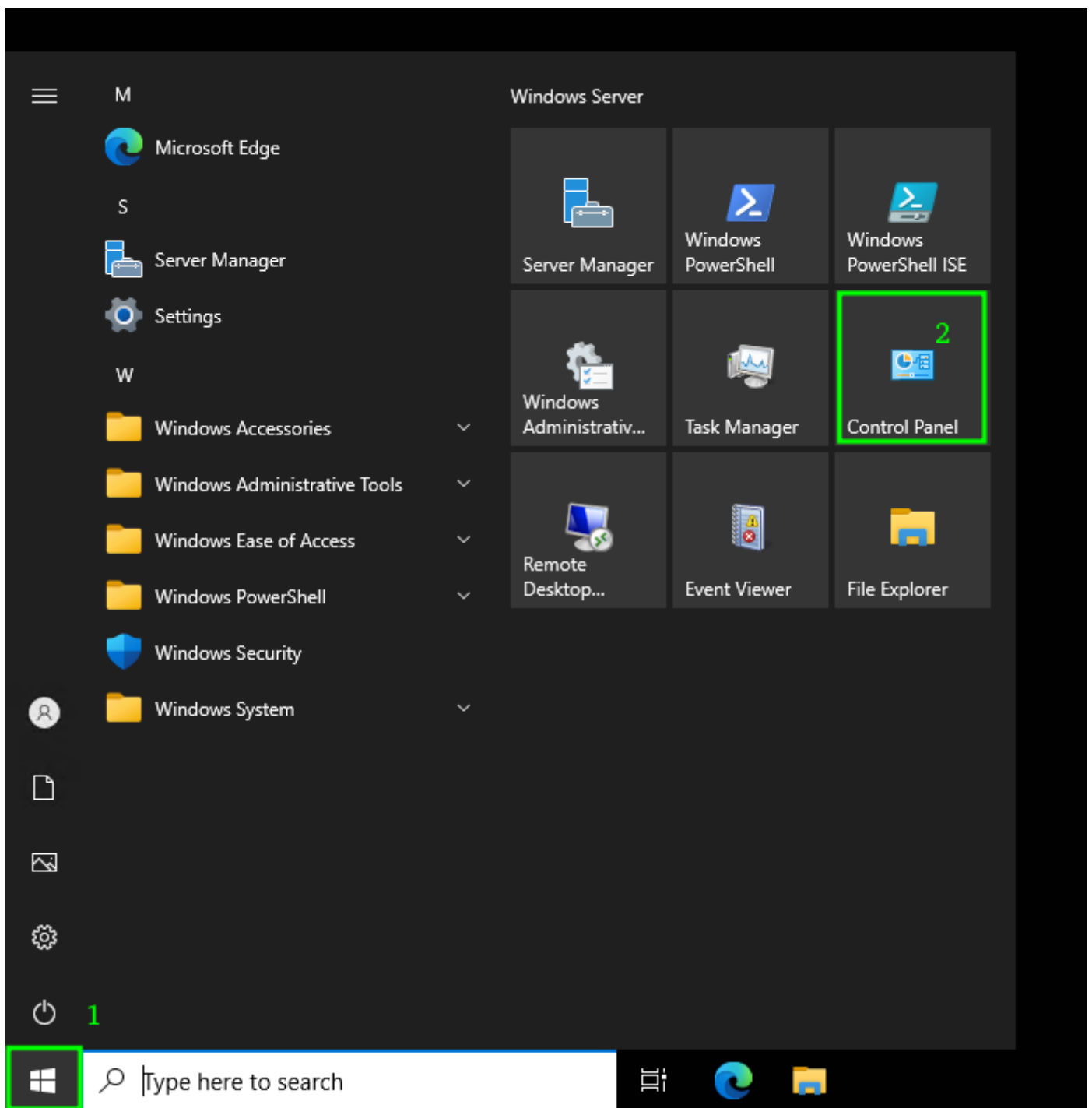
Брандмауэр (Firewall) в windows представляет собой набор правил. Правило это описание разрешения или запрета соединения. Они могут быть входящими и исходящими, регулирующими доступ к этому компьютеру или с этого компьютера в сеть.

Например, если хотите чтобы Ваш сайт был доступен из внешней сети, необходимо настроить правило Firewall.

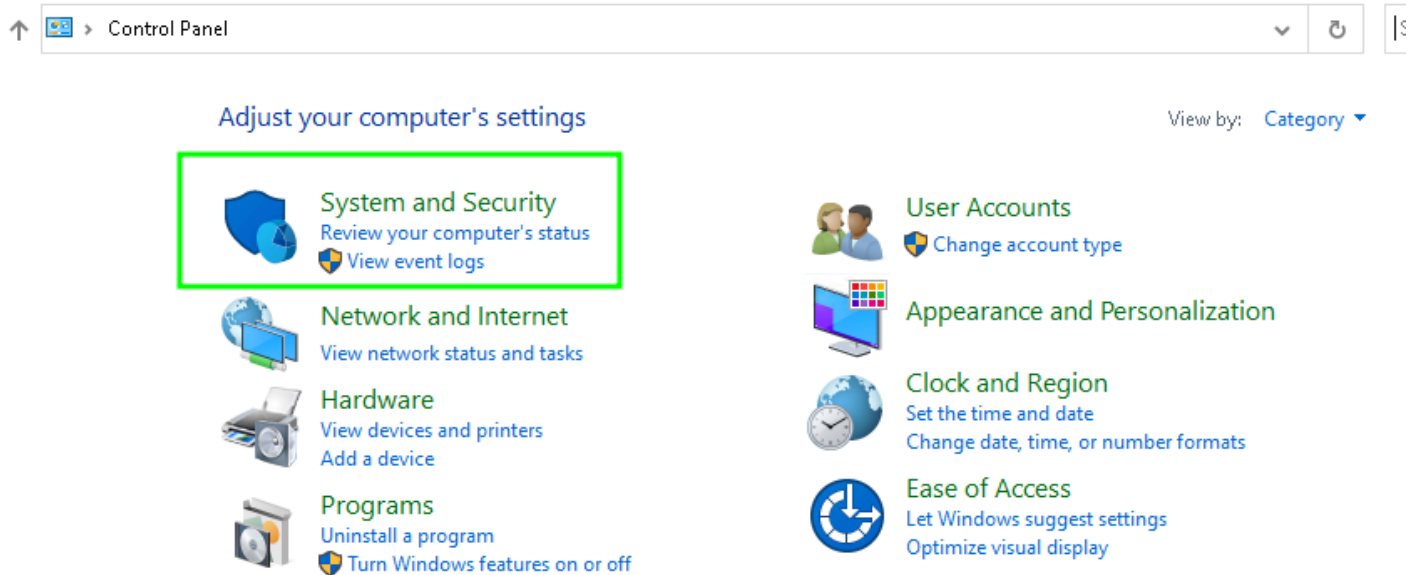
Данная инструкция написана для Windows Server 2022. Для других версий ОС Windows она также применима.

Для настройки правила сделайте следующее:

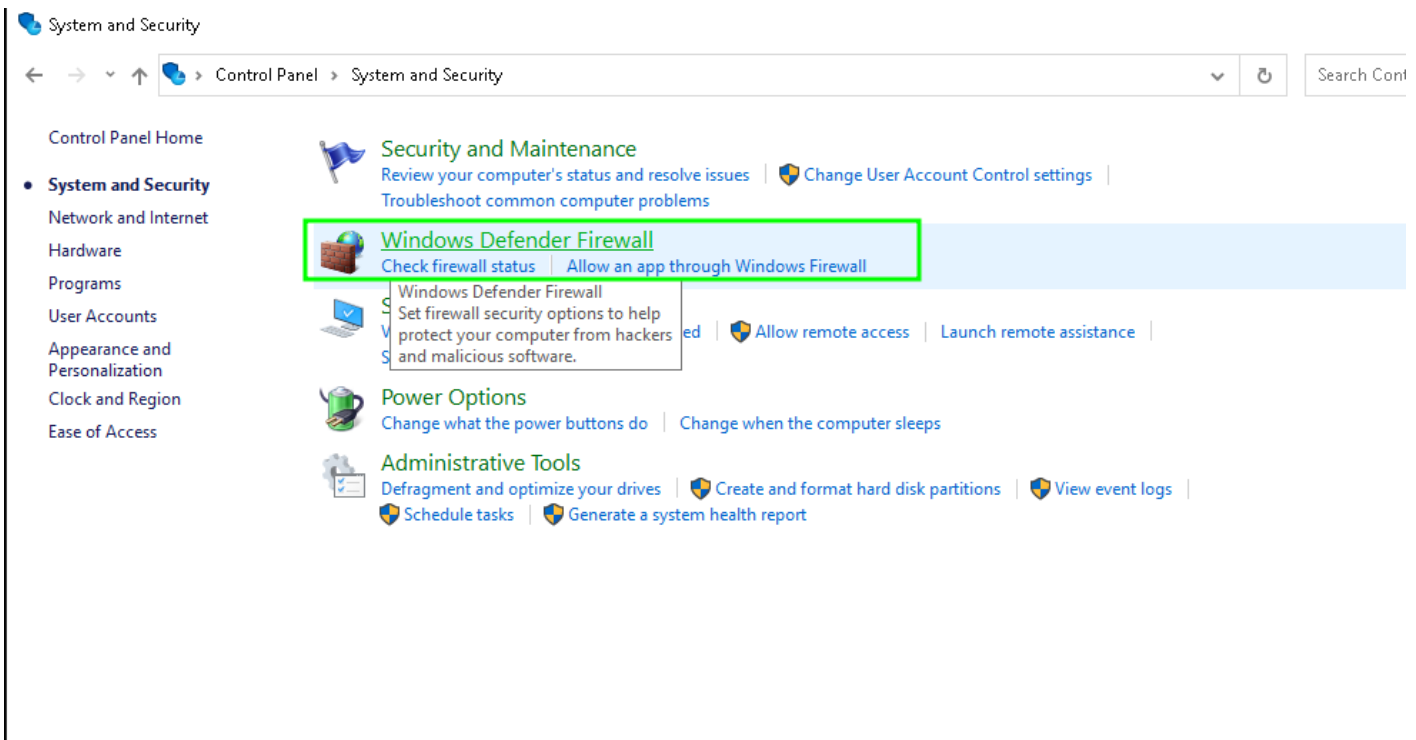
1. Подключитесь к своему серверу и нажмите "Пуск" - "Панель управления(Control Panel)".



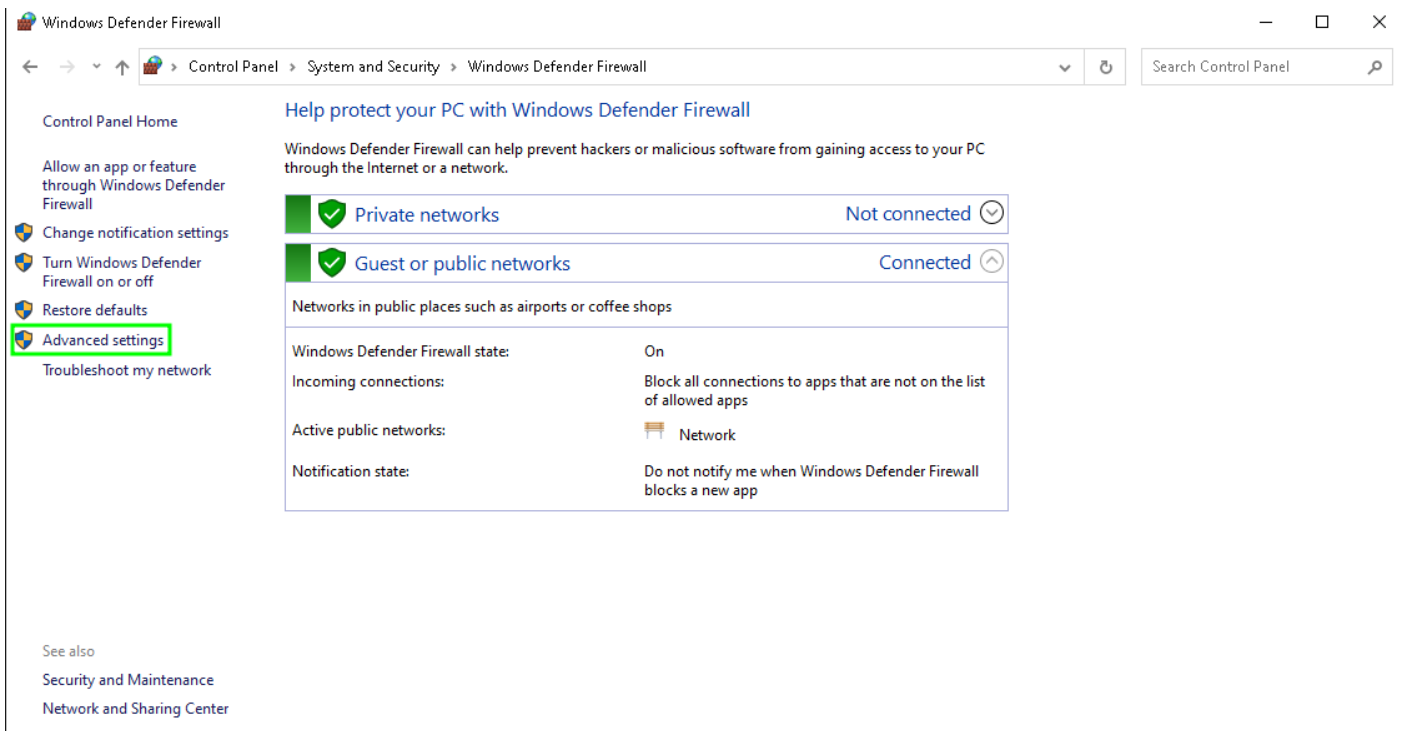
2. Выберите раздел "Система и безопасность(System and Security)"



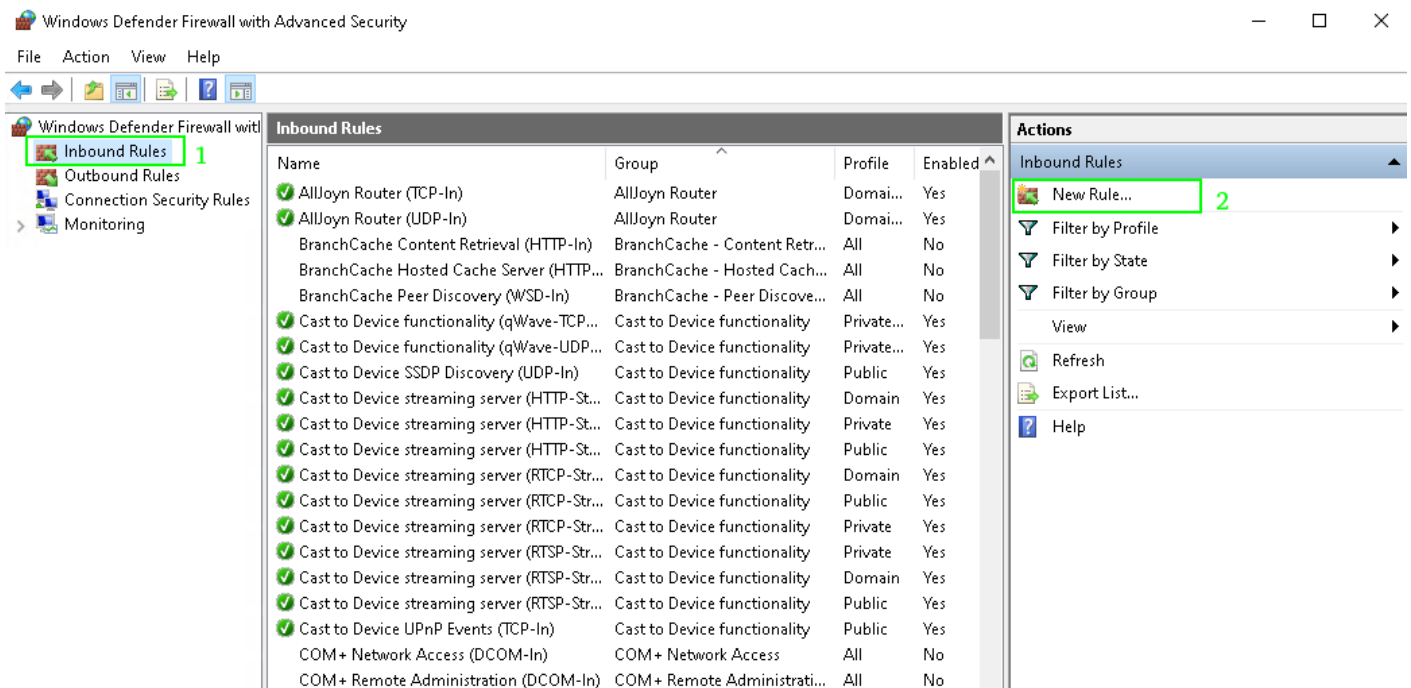
3. Выберите раздел "Брандмауэр Windows" (Windows Defender Firewall)



4. В столбце слева выберите Дополнительные параметры(Advanced settings)



5. В открывшемся окне перейдите в раздел “Правила для входящих подключений”(Inbound Rules), после чего нажмите “Создать правило”(New Rule).



6. Создадим правило для порта 80, также можно создать правило для конкретной программы или использовать стандартное правило для стандартных служб Windows. Можно также создать полностью настраиваемое правило под Ваши нужды.

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- 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:**

AllJoyn Router

Rule that controls connections for a Windows experience.

☐ **Custom**

Custom rule.

< Back

Next >

Cancel

7. Выберем тип протокола для фильтрации трафика, это может быть либо tcp либо udp, порт может быть любой или вообще можно открыть-закрыть все порты. В нашем примере мы откроем 80 порт для протокола tcp.

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:

80

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

8. Далее определим, что именно должно делать правило - разрешать или запрещать трафик по указанным нами на предыдущем шаге портам. Мы разрешим трафик в нашем примере.

Action

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

Steps:

- Rule Type
- Protocol and Ports
- 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

9. Укажем для какой сети должно применяться это правило. Доменной, частной или публичной. Если Вы не знаете, какую выбрать, выберите все три.

New Inbound Rule Wizard

×

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- 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

10. На последнем шаге задайте имя правила и описание(если необходимо).

New Inbound Rule Wizard

×

Name

Specify the name and description of this rule.

Steps:

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

Name:

allow 80 port

Description (optional):

allow 80 port

< Back

Finish

Cancel

11. Готово. Теперь данный порт открыт. В списке "Правил для входящих подключений" мы можем увидеть только что созданное правило.

Windows Defender Firewall with Advanced Security

FileActionViewHelp

Windows Defender Firewall

Inbound Rules

Outbound Rules

Connection Security Rules

Monitoring

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
allow 80 port		All	Yes	Allow	No	Any	Any	Any	TCP
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes	Allow	No	%System...	Any	Any	UDP
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP
BranchCache Hosted Cache Server (HTTP-In)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP
Cast to Device functionality (qWave-TCP-In)	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP-In)	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Any	TCP
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local subnet	TCP
Cast to Device streaming server (HTTP-Str...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	TCP
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	TCP
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo Renderers	TCP
COM+ Network Access (DCOM-In)	COM+ Network Access	All	No	Allow	No	%system...	Any	Any	TCP
COM+ Remote Administration (DCOM-In)	COM+ Remote Administrati...	All	No	Allow	No	%system...	Any	Any	TCP
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMP
Core Networking - Destination Unreachab...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMP
Core Networking - Dynamic Host Configur...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configur...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Internet Group Manag...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	TCP
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPV6
Core Networking - Multicast Listener Disc...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMP
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMP
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMP
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	No	System	Any	Local subnet	ICMP

Inbound Rules

New ...

Filter ...

Filter ...

Filter ...

View

Refresh

Export...

Help

allow 80 p...

Disabl...

Cut

Copy

Delete

Prope...

Help

Версия #1

Кирилл создал 23 января 2024 09:29:47

Кирилл обновил 23 января 2024 10:08:35