

Используя **брандмауэр** неуправляемого клиента **Symantec Endpoint Protection** вы без труда сможете запретить определенной программе доступ в Интернет.

## Запрещаем программе доступ в Интернет через Symantec Endpoint Protection

Откройте антивирусную программу, в разделе "**Предупреждение последствий использования эксплойтов сети и хоста**" нажмите "**Параметры**".





Бесплатное обновление Windows 7 до Windows 10



Скачать Windows 11 версии 23Н2

## ОБСУЖДАЕМЫЕ СТАТЬИ





В появившемся окне кликните "Настроить правила брандмауэра".

	Изменить параметры Показать журналы
	Показать параметры приложений Показать сетевые операции
	Настроить правила брандмауэра
	Выключить предупреждение последствий использования эксплойтов памяти
	Выключить функцию Защита от сетевых угроз

Нажмите кнопку "Добавить".

Настроить правила брандмауэра			Х
Правила брандмауэра разрешают, блокируют и регистрируют в журн	але сетевой трафи	к.	
Имя правила	Хосты	Порты и протоколы	Д ^
Блокировать пакеты IPv6 (тип Ethemet 0x86dd)	Все хосты	Тип Ethemet 34525; входящий и ис	Бл
Запретить передачу пакетов IPv6 по протоколу IPv4 (Teredo) ч	Все хосты	Удаленные порты UDP 3544; вход	Б
Block IPv6 over IPv4 (ISATAP)	Все хосты	Протокол IP типа 41; входящий и и	Бл
Allow common ICMPv6 traffic	Все хосты	Тип ІСМРV6: 1-4,128-132,135,136,1	Pa
Разрешить беспроводной трафик EAPOL	Все хосты	Тип Ethemet 0x888E; входящий и и	Pa
Allow BOOTP protocol	Все хосты	Покальные порты UDP 68,67; вход	Pa
Allow UPnP Discovery from private IPv4 addresses	10.0.0.10.255	Покальные порты UDP 1900; вход	Pa
Allow UPnP Discovery from private IPv6 addresses	fc00::-fdff.ffff.ffff:	Покальные порты UDP 1900; вход	Pa
Block UPnP Discovery	Все хосты	Покальные порты UDP 1900; вход	Бл
Allow Web Service requests from private IPv4 addresses part A	10.0.0.0-10.255	Покальные порты ТСР 5357,5358;	Pa
Allow Web Service requests from private IPv6 addresses part A	fc00::-fdff.ffff.ffff:	Покальные порты ТСР 5357,5358;	Pa
Allow Web Service requests from private IPv4 addresses part B	10.0.0.10.255	Покальные порты UDP 5357,5358;	Pa
Allow Web Service requests from private IPv6 addresses part B	fc00::fdff.ffff.ffff:	Покальные порты UDP 5357,5358;	Pa
✓ Block Web Service requests part A	Все хосты	Локальные порты ТСР 5357,5358;	Бı ~ >
Добавить Изменить Удалить 1			
		ОК Отмена Справк	a

Задайте имя правила, например "**Программы**", проверьте что отмечен пункт "**Блокировать этот трафик**".

	Kaspersky Standard для Windows - бесплатная лицензия
	2024-02-04
۲	Realtek ALC1200 - подробности и отличия от более качественного аудиокодека ALC1220-VB
	2021-02-09
	Как включить русский язык в Microsoft Edge на основе Chromium
	2019-07-11
	Kerish PC Doctor - бесплатная лицензия на 1 год
	2024-02-19

## ОПРОС

## Ваш антивирус?

- Безопасность Windows
- ESET NOD32
- Bitdefender
- Kaspersky
- Comodo
- McAfee
- Dr.Web
- Norton
- Panda
- Avast
- Avira
- AVG
- Другой



🕛 Добав	вить правило брандмауэра		×
Общие	Хосты Порты и протоколы Приложения Расписание		
Имя п	правила		
Прог	граммы		
Dežes	TT-1/2		_
Деист	локировать этот трафик О Разрешить этот тра	фик	
Парам	метры брандмауэра		
Прим	иенять правило к следующему сетевому адаптеру:		
Bce	сетевые адаптеры		1
Прим	иенять правило во время экранной заставки:		
Вкл.	. или Выкл.		1
Pe	егистрировать трафик в журнале пакетов		
Сведен Блокир трафик следую	ния о правиле: зовать входящий и исходящий трафик из/в: Все хосты. При су следующих протоколов и портов: Все типы протокола IP эщих сетевых адаптеров: Все сетевые адаптеры.	меняется к . Для	~ ~
	ОК Отм	ена Сп	равка

Убедитесь что в меню "Порты и протоколы" выбрано "Все протоколы IP" и направление "Оба".

🔰 Добав	зить пра	вило брандмауэра			×
Общие	Хосты	Порты и протоколы	Приложения	Расписание	
Прим	енять пр	авило к			
Про	токол:	Все протоколы	IP	$\sim$	
Han	равление	е Оба		~	
Сведен Блокир	ния о пра ровать вх	виле: кодящий и исходящий	трафик из/в: В	се хосты. Применяется	к
трафик следую	ку следую ощих сете	ощих протоколов и пор евых адаптеров: Все с	ртов: Все типы сетевые адапте	протокола IP. Для ры.	
					~
			OK	Отмена	Справка

Перейдите в "Приложения", добавьте нужную программу через кнопку "Обзор" и нажмите "ОК".

	ОТОКОЛЫ	риложения га	списание	
Приложения:		Показать тольн	ю выбранные пр	иложения
Приложение	Версия	Путь		
CPU-Z Application	1.8.6.0	C:\Program	Files\CPU-Z\cpu	ız_x64.exe
<				>
Выбрать все	Отме	нить все	Обзо	p
	x64.exe			
Путык приложению. C:\Program Files\CPU-Z\couz				~
Type к приложению. C:\Program Files\CPU-Z\cpuz Сведения о правиле:				
туть к приложению. С:\Program Files\CPU-Z\cpuz Сведения о правиле: Блокировать входящий и ис	ходящий тра	фикиз/в:Все х	осты. Применяет	тся к
туть к приложению. C:\Program Files\CPU-Z\cpuz Сведения о правиле: Блокировать входящий и ис графику следующих протокк следующих сетевых адаптер	ходящий тра олов и порто оов: Все сете	фик из/в:Все х в:Все типы про вые адаптить	осты. Применяе токола IP. Для	тся к
пуль к приложению. С:\Program Files\CPU-Z\cpuz Сведения о правиле: Блокировать входящий и ис трафику следующих протокк спедующих сетевых адапте Это правило влияет на след	ходящий тра олов и порто оов: Все сете ующие прило	фик из/в:Все ж в:Все типы про вые адаптеры. ожения:СРU-Z А	осты. Применяе токола IP. Для opplication.	тся к

В настройках правил брандмауэра найдите только что созданное правило, поднимите его в самый вверх используя стрелочку и нажмите "**OK**".

не сетевой трафик (осты Все хосты Все хосты Сее хосты Сее хосты Все хосты Все хосты		Д ^ Бл Бл
Косты Все хосты Все хосты Все хосты Все хосты Все хосты	Порты и протоколы Все типы протокола IP; входящий Тип Ethemet 34525; входящий и ис Удаленные порты UDP 3544; вход Протокол IP типа 41; входящий и и	Д ^ Бі Бі
Все хосты Все хосты Все хосты Все хосты Все хосты Все хосты	Все типы протокола IP; входящий Тип Ethemet 34525; входящий и ис Удаленные порты UDP 3544; вход Протокол IP типа 41; входящий и и	Б Бл Бл
Все хосты Все хосты Все хосты Все хосты	Тип Ethemet 34525; входящий и ис Удаленные порты UDP 3544; вход Протокол IP типа 41; входящий и и	Бі
Все хосты Все хосты Все хосты	Удаленные порты UDP 3544; вход Протокол IP типа 41; входящий и и	Б
Все хосты Все хосты	Протокол IP типа 41; входящий и и	
Все хосты		Бл
	Тип ІСМРV6: 1-4,128-132,135,136,1	Pa
все хосты	Тип Ethernet 0x888E; входящий и и	Pa
Все хосты	Локальные порты UDP 68,67; вход	Pa
0.0.0.0-10.255	Локальные порты UDP 1900; вход	Pa
c00::-fdff.ffff.ffff:	Локальные порты UDP 1900; вход	Pa
Все хосты	Локальные порты UDP 1900; вход	Бл
0.0.0.0-10.255	Локальные порты ТСР 5357,5358;	Pa
c00::-fdff.ffff.ffff:	Локальные порты ТСР 5357,5358;	Pa
0.0.0.0-10.255	Покальные порты UDP 5357,5358;	Pa
c00::-fdff.ffff.ffff:	Локальные порты UDP 5357,5358;	Pi ⊻
		>
	ОК Отмена Справк	a
	е хосты е хосты е хосты 00.0-10.255 10.:4dff ffff ffff е хосты 0.0.0-10.255 10::4dff ffff ffff 0.0.0-10.255 10::4dff ffff ffff fff	е хосты Тип ICMPV6: 1-4,128-132,135,136,1 е хосты Тип Ethemet 0x888E; входящий и и е хосты Покальные порты UDP 68,67; вход 00.0-10.255 Покальные порты UDP 1900; вход 0.0.0-10.255 Покальные порты UDP 1900; вход 0.0.0-10.255 Покальные порты UDP 1900; вход 0.0.0-10.255 Покальные порты UDP 5357,5358; 00:-4dff ffff fffff Покальные порты UDP 5357,5358;

Заметьте, что в это правило можно добавить сколько угодно программ, используя кнопку "Изменить" и блокировать им интернет-соединения через брандмауэр Symantec Endpoint Protection.



Рекомендуемый контент