Тема: Настройка межсетевого экрана в Windows 10

Цель: Ознакомиться с встроенным в Windows межсетевым экраном.

Межсетевой экран (брандмауэр, файервол) предназначен для повышения безопасности системы при работе в сети, он ограждает сеть от внешних вредоносных атак, не пропускает «опасный» входящий и исходящий трафик и блокирует подозрительную активность.

• Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решение: пропустить или блокировать конкретный трафик.

• Межсетевые экраны используются в качестве первой линии защиты сетей уже более 25 лет.

• Они ставят барьер между защищенными, контролируемыми внутренними сетями, которым можно доверять, и ненадежными внешними сетями, такими как Интернет.

• Межсетевой экран может быть аппаратным, программным или смешанного типа.

Типы межсетевых экранов

Межсетевой экран на прокси-сервере

Это один из первых типов МСЭ. Межсетевой экран на прокси-сервере служит шлюзом между сетями для конкретного приложения. Проксисерверы могут выполнять дополнительные функции, например кеширование контента и его защиту путем предотвращения прямых подключений из-за пределов сети. Однако это может отрицательно сказаться на пропускной способности и производительности поддерживаемых приложений.

Межсетевой экран с контролем состояния сеансов

Он пропускает или блокирует трафик с учетом состояния, порта и протокола. Он отслеживает все действия с момента открытия соединения до его закрытия. Решения о фильтрации принимаются на основании как правил, определяемых администратором, так и контекста. Под контекстом понимается информация, полученная из предыдущих соединений и пакетов, принадлежащих данному соединению.

Межсетевой экран нового поколения (NGFW)

Современные межсетевые экраны не ограничиваются фильтрацией пакетов и контролем за состоянием сеансов. Большинство компаний внедряет межсетевые экраны нового поколения, чтобы противостоять

современным угрозам, таким как сложное вредоносное ПО и атаки на уровне приложений.

Настройка брандмауэра в Windows 10

В отличие от сторонних (особенно бесплатных) программ, брандмауэр Windows довольно легок в управлении, имеет дружественный интерфейс и понятные настройки.

Встроенный брандмауэр не имеет рекламы и не требует платной активации. Брандмауэр работает в фоновом режиме беспрерывно и не может отключиться без команды пользователя. В случае если приложению потребуется доступ к определённым параметрам компьютера, придёт запрос от файервола, который нужно будет подтвердить.

Работа по настройке начинается из классической «Панели управления» Windows.

1. Вызываем меню «Выполнить» комбинацией клавиш Windows+R и вводим команду

control

📨 Выполн	ить Х
	Введите имя программы, папки, документа или ресурса Интернета, которые требуется открыть.
<u>О</u> ткрыть:	control
	ОК Отмена Об <u>з</u> ор

2. Переключаемся на режим просмотра «Мелкие значки» и находим апплет «Брандмауэр защитника Windows».



Типы сетей

Различают два типа сетей: частные и общественные. Первыми считаются доверенные подключения к устройствам, например, дома или в офисе, когда все узлы известны и безопасны. Вторыми – соединения с внешними источниками через проводные или беспроводные адаптеры. По умолчанию общественные сети считаются небезопасными,

и к ним применяются более строгие правила.



Включение и отключение, блокировка, уведомления

Активировать брандмауэр или отключить его можно, перейдя по соответствующей ссылке

в разделе настроек:



Здесь достаточно поставить переключатель в нужное положение и нажать ОК.



Блокировка подразумевает запрет всех входящих подключений, то есть любые приложения, в том числе и браузер, не смогут загружать данные из сети.

💮 Настроить параметры				-		×
← → → ↑ 🔗 « Брандмауэр	защитника Windows > Настроить параметры	~ Ö	Поиск в па	анели управ	ления	P
 	защитника Windows > Настроить параметры а параметров для каждого типа сети изменить параметры брандмауэра для каждого из используемых тиг для частной сети Включить брандмауэр Защитника Windows □ Блокировать все входящие подключения, в том числе для прило списке разрешенных программ Уведомлять, когда брандмауэр Защитника Windows (не рекомендуется) для общественной сети Включить брандмауэр Защитника Windows □ Блокировать все входящие подключения, в том числе для прило списке разрешенных программ Уведомлять, когда брандмауэр Защитника Windows □ Блокировать все входящие подключения, в том числе для прило списке разрешенных программ ○ Уведомлять, когда брандмауэр Защитника Windows □ Блокировать все входящие подключения, в том числе для прило списке разрешенных программ ○ Уведомлять, когда брандмауэр Защитника Windows □ Блокировать все входящие подключения, в том числе для прило списке разрешенных программ ○ Уведомлять, когда брандмауэр Защитника Windows (не рекомендуется) ○ Уведомлять, когда брандмауэр Защитника Windows (не рекомендуется) ○ Толючить брандмауэр Защитника Windows (не рекомендуется)	 С тов сетей. жений, ука овое прило жений, ука овое прило 	ззанных в ожение	анели управ	ления	
		ОК	Отмена			

Уведомления представляют собой особые окна, возникающие при попытках подозрительных программ выйти в интернет или локальную сеть.

🔗 Оповещение	системы безо	пасности Windows	\times
Бранд прило	мауэр Win жения	dows заблокировал некоторые функции эт	ого
Брандмауэр Windo во всех обществе	ws заблокиров нных и частны	ал некоторые функции Bitcoin Knots (GUI node for Bitcoin) х сетях.	
	Имя:	Bitcoin Knots (GUI node for Bitcoin) Bitcoin	
Ť	издатель. Путь:	C:\program files\bitcoin\bitcoin-qt.exe	
Это приложение п брандмауэра.	ытается получ	ить сведения непосредственно из Интернета, возможно, в	обход
Разрешить Bitcoin	Knots (GUI nod ти, например, J	e for Bitcoin) связь в этих сетях: 10машняя или рабочая сеть	
Обществен так как так	ные сети, напр ие сети зачаст	имер в аэропортах и кафе (не рекомендуется, ую защищены недостаточно или не защищены вовсе)	
Что может случит	ься, если разр	ешить взаимодействие с приложением через брандмауэр?	
		Разрешить доступ Отмен	Ia

Функция отключается снятием флажков в указанных чекбоксах.



Сброс настроек

Данная процедура удаляет все пользовательские правила и приводит параметры к значениям по умолчанию.



Сброс обычно производится при сбоях в работе брандмауэра в силу различных причин, а также после неудачных экспериментов с настройками безопасности. Следует понимать, что и «правильные» опции также будут сброшены, что может привести к неработоспособности приложений, требующих подключения к сети.

💮 Восстановить значения	по умолчанию		- 0	×
🔶 🔶 👻 🛧 🔗 « Бр	андмауэр Защитника Windo > Восстановить значения по умолчанию	~ Ō	Поиск в панели управления	Q
BC The Ball	андиву р защиника чиниси. У восстановить значения по умолчанию осстановлении параметров по умолчанию будут удалены все параметры бри щитника Windows, которые вы задали для всех сетевых расположений. Это мож рушению работоспособности некоторых приложений. Восстановить значения по умолчанию	андмауз	ра ести к	~
			Отмена	

Взаимодействие с программами

Данная функция позволяет разрешить определенным программам подключение к сети для обмена данными.



Этот список еще называют «исключениями».

Разрешение обмена данными с приложениями в брандм Windows Чтобы абазить изменить или ударить разрешенные рамоожения и ролт	ауэре За	щитника	
чтобы добавите, измените или удалите разрешенные приложения и порт параметры". Что может случиться, если разрешить обмен данными с приложением?	• Целкнин	енить параметры	
<u>Р</u> азрешенные программы и компоненты:			
Название	Частная	Публичная 🔺	
Advego Plagiatus			
✓ BlueStacks Service	\checkmark	✓	
BranchCache - клиент размещенного кэша (используется HTTPS)			
BranchCache - обнаружение кэширующих узлов (использует WSD)			
BranchCache - получение содержимого (использует HTTP)			
BranchCache - сервер размещенного кэша (используется HTTPS)			
Cobian backup 11 Gravity - Interface		✓	
☑ DiagTrack	\checkmark	✓	
Divinity Original Sin 2		✓	
EBook Codec Downloader	\checkmark	✓	
EBook Codec Downloader	\checkmark		
✓ Firefox (C:\Program Files (x86)\Mozilla Firefox)	~	<u> </u>	
	Сведе <u>н</u> ия	У <u>да</u> лить	
Page	шить друго	е приложение	
(upp of	. <u></u>	- opposition content	

Правила

Правила – это основной инструмент брандмауэра для обеспечения безопасности. С их помощью можно запрещать или разрешать сетевые подключения. Эти опции располагаются в разделе дополнительных параметров.



Входящие правила содержат условия для получения данных извне, то есть загрузки информации из сети (download). Позиции можно создавать для любых программ, компонентов системы и портов. Настройка исходящих правил подразумевает запрет или разрешение отправки запросов на сервера и контроль процесса «отдачи» (upload).

айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка								
• 🔿 🙍 📷 🗟 👔 📷								
	Правила для входящих по	одключени	й					Действия
Правила для входящих подключений	1мя	Fpynna	Профиль	Включено	Действие	Частота	Пр ^	Правила д.
Правила для исходящего подключен	Общий доступ к файла	Общий	Общий	Да	Разрешить	Нет	Sys	🕅 Созда
аблюзение	Общий доступ к файла	Общий	Домен	Нет	Разрешить	Нет	Svs	
la shi qeni e	Общий доступ к файла	Общий	Частный	Нет	Разрешить	Нет	Sys	у филь
	Общий доступ к файла	Общий	Частный	Нет	Разрешить	Нет	Sys	🍸 Филь
	Общий доступ к файла	Общий	Домен	Нет	Разрешить	Нет	Svs	🍸 Филь
	💋 Общий доступ к файла	Общий	Общий	Да	Разрешить	Нет	Sys	Вил
	💋 Общий доступ с помо	Общий	Bce	Дa	Разрешить	Нет	%S	D and
	Оптимизация доставки	Оптими	Bce	Дa	Разрешить	Нет	%S	Обно.
	Оптимизация доставки	Оптими	Bce	Да	Разрешить	Нет	%S	🔒 Экспо.
	Основы сетей - IPHTTP	Основы	Bce	Дa	Разрешить	Нет	Sys	Cnpa
	🗿 Основы сетей — IPv6 (в	Основы	Bce	Дa	Разрешить	Нет	Svs	- cupun
	Основы сетей — RA (вх	Основы	Bce	Да	Разрешить	Нет	Svs	
	🗿 Основы сетей - Teredo (Основы	Bce	Да	Разрешить	Нет	%S	
	Основы сетей - заверш	Основы	Bce	Да	Разрешить	Нет	Svs	
	Основы сетей — запрос	Основы	Bce	Да	Разрешить	Нет	Svs	
	Основы сетей — запрос	Основы	Bce	Ла	Разрешить	Нет	Svs	
	Основы сетей — запрос	Основы	Bce	Да	Разрешить	Нет	Svs	
	🗿 Основы сетей — назнач	Основы	Bce	Ла	Разрешить	Нет	Svs	
	Основы сетей - назначе	Основы	Bce	Да	Разрешить	Нет	Svs	
	🗿 Основы сетей — объяв	Основы	Bce	Да	Разрешить	Нет	Sve	
		Основы	Bce	Да	Разрешить	Her	Sve	
	Основы сетей - отчет м	Основы	Rce	Да	Разрешить	Нет	Sve	
	Основы сетей — оцибк	Основы	Bce	Ла	Разрешить	Нет	Sve	
	Основы сетей — розвы	Основы	Bce	Ла	Разрешить	Her	Svs	
	Основы сетей - проток	Основы	Ree	Ла	Разрешить	Нет	%6	
	Основы сетей - проток	Основы	Ree	0.	Разрешить	Her	~~~	
	Основы сетей - проток	Основы	Ree	н ^а Ла	разрешить	Her	Swe	
	Посновы сетей — прото	Основы	Rea	A.	Разрешить	Har	Sur	
		Паатфо	06000	Да Ла	Разрешить	Her	9/5 9/5	
		Πeerde	Лениен Ц	A*	Разрешить	Here	200	
	Партформа подключен	Dearthe	Домен, Ч	Да	Разрешить	Har	/03 9/ S	
	и платформа подключен	платфо	домен, ч	дd Цаа	- азрешить Посто	Lier Lier	263 97 D	
	г проигрыватель Windo	проигр	DCE	nei	назрешить	mei	/or V	

Правила безопасности позволяют производить подключения с использованием IPSec – набора специальных протоколов, согласно которым проводится

айл Действие Вид Справка									
	1						_		
нитор брандмауэра Защитника Windov	Правила для входящих по	дключени	й					Действия	
Правила для входящих подключении	Имя	Группа	Профиль	Включено	Действие	Частота	Пр ^	Правила д	
Правида безодасности доаклюцения	🗿 Общий доступ к файла	Общий	Общий	Дa	Разрешить	Нет	Sys	🛃 Созда	
арлюление	Общий доступ к файла	Общий	Домен	Нет	Разрешить	Нет	Sys		
a serie de la constance	Общий доступ к файла	Общий	Частный	Нет	Разрешить	Нет	Sys	и филь	
	Общий доступ к файла	Общий	Частный	Нет	Разрешить	Нет	Sys	🛛 🖓 Филь	
	Общий доступ к файла	Общий	Домен	Нет	Разрешить	Нет	Sys	🕎 Филь	
	💋 Общий доступ к файла	Общий	Общий	Да	Разрешить	Нет	Sys	Вид	
	💋 Общий доступ с помо	Общий	Bce	Да	Разрешить	Нет	%S		
	🔮 Оптимизация доставки	Оптими	Bce	Да	Разрешить	Нет	%S	С Обно	
	💋 Оптимизация доставки	Оптими	Bce	Да	Разрешить	Нет	%S	📑 Экспо	
	Ӯ Основы сетей - IPHTTP	Основы	Bce	Да	Разрешить	Нет	Sys	Спра	
	Ӯ Основы сетей — IPv6 (в	Основы	Bce	Да	Разрешить	Нет	Sys	- ·	
	Ӯ Основы сетей — RA (вх	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей - Teredo (Основы	Bce	Да	Разрешить	Нет	%S;		
	Ӯ Основы сетей - заверш	Основы	Bce	Да	Разрешить	Нет	Sys		
	🔮 Основы сетей — запрос	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей — запрос	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей — запрос	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей — назнач	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей - назначе	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей — объяв	Основы	Bce	Да	Разрешить	Нет	Sys		
	Ӯ Основы сетей - отчет м	Основы	Bce	Да	Разрешить	Нет	Sys		
	🔮 Основы сетей - отчет м	Основы	Bce	Да	Разрешить	Нет	Sys		
	🔮 Основы сетей — ошибк	Основы	Bce	Да	Разрешить	Нет	Sys		
	💋 Основы сетей — превы	Основы	Bce	Да	Разрешить	Нет	Sys		
	🔮 Основы сетей - проток	Основы	Bce	Да	Разрешить	Нет	%Sj		
	🔮 Основы сетей - проток	Основы	Bce	Да	Разрешить	Нет	%S		
	Ӯ Основы сетей — прото	Основы	Bce	Да	Разрешить	Нет	Sys		
	🔮 Основы сетей — слишк	Основы	Bce	Да	Разрешить	Нет	Sys		
	🗿 Платформа подключен	Платфо	Общий	Да	Разрешить	Нет	%S;		
	🔮 Платформа подключен	Платфо	Домен, Ч	Да	Разрешить	Нет	%S		
	Платформа подключен	Платфо	Домен, Ч	Да	Разрешить	Нет	%S		
	Проигрыватель Windo	Проигр	Bce	Нет	Разрешить	Нет	%P ↓		
>	<						>		

аутентификация, получение и проверка целостности полученных данных и их шифрование, а также защищенная передача ключей через глобальную сеть.

В ветке «**Наблюдение**», в разделе сопоставления, можно просматривать информацию о тех подключениях, для которых настроены правила безопасности.

🝻 Монитор брандмауэра Защитника Wir	ndows в режиме повышенной безопасности —	o x
<u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка		
🗢 🔿 🙍 🖬 🔒 📓 🖬		
🔗 Монитор брандмауэра Защитника Wi	Сопоставления безопасности	Действия
🗱 Правила для входящих подключен	Има	Сопостав 🔺
Правила для исходящего подключ	Основной режим	Вид
Наблюдение	Быстрый режим	
рандмауэр	_ · ·	зуружено
		Cnpa
Сопоставления безопасности		
Основной режим		
выстрый режим		
< >>		1

Профили

Профили представляют собой набор параметров для разных типов подключений. Существуют три их типа: «Общий», «Частный» и «Профиль домена».



При обычной работе эти наборы активируются автоматически при соединении с определенным типом сети (выбирается при создании нового подключения или подсоединении адаптера – сетевой карты).

Задание:

- 1. Ознакомиться с настройками встроенного брандмауэра Windows;
- 2. Используя интернет-ресурс <u>https://lumpics.ru/firewall-settings-in-windows-10/</u> самостоятельно изучить вопросы создания правил для программ, работу с исключениями, правила для портов.
- 3. Ответить на вопросы:
 - что такое межсетевой экран?
 - какие типы межсетевых экранов существуют?
 - как настроить межсетевой экран в Windows 10?