

Настройка сетевого экрана в OC Windows для подключений из сети за VPN-сервером Keenetic

В предлагаемой согласно статье Базы знаний <u>http://zyxel.ru/kb/4214</u> схеме объединения локальных сетей, доступ из сети за сервером к хостам в сети за клиентом РРТР может быть заблокирован политиками по умолчанию на файерволе. К примеру в операционной системе Windows по умолчанию блокируются входящие подключения (в том числе и зондирование ICMP), если адрес источника этого подключения не принадлежит к назначенной на интерфейсе компьютера сети.

Это означает, что Компьютер будет иметь доступ к USB-принтеру и хранилищу NAS, но на Ноутбуке обращения от него отбрасываются без соответствующей настройки сетевого экрана.

И наоборот, при обращении ноутбука из сети за ИЦ1 (VPN-клиентом) к Windows-компьютеру в сети за сервером ИЦ2, будет выполнена трансляция адреса NAT и действительный адрес отправителя сменится на адрес ИЦ2 полученный от сервера PPTP. То есть, обращение НЕ придёт от адреса хоста в той же сети, что и адрес назначения — и будет заблокировано брандмауэром Windows.

В обратном направлении, адрес отправителя входящего в сеть за ИЦ1 пакета (от Компьютера к Ноутбуку) не подменяется. Однако условие для блокировки по умолчанию на файерволе ноутбука снова выполняется — отправленный от 192.168.1.33 к 192.168.2.33 пакет будет

сброшен на компьютере 192.168.2.33.

Рассмотрим настройку Брандмауэра Windows, разрешающую подключения из удалённой сети к компьютерам в локальной сети. Для этого достаточно создать политику сетевого экрана, регулирующую входящие подключения.

Приведённые далее скриншоты выполнены в операционной системе Windows 7.





1. В строке командной строки Windows (*Win+R*) выполните команду *wf.msc* Откроется окно апплета конфигурации службы Windows. Это же окно можно открыть через

меню Панель управления — Система и безопасность — Брандмауэр Windows по кнопке Дополнительные параметры.



2. Выбрав в списке слева пункт **Правила для входящих подключений**, для добавления правила обработки трафика нужно нажать в правой панели **Создать правило..**.

👷 Брандмауэр Windows в режиме повышенной безопасности				- • • ×			
Файл Действие Вид Справка							
Брандмауэр Windows в режик	Правила для входящих подключении		_	Действия			
Правила для входящих по,	Имя	Группа	Профил 📩	Правила для входящих подключений	^		
Правила безопасности по	🔘 Обнаружение кэширующих узлов Bran	BranchCache - обнаружен	Bce	🗱 Создать правило			
Наблюдение	🔘 Получение содержимого BranchCache	BranchCache - получение	Bce	Фильтровать по профилю	•		
	🔘 Сервер размещенного кэша BranchCa	BranchCache - сервер разм	Bce ≡				
	Secure Socket Tunneling Protocol (SSTP	Secure Socket Tunneling Pr	Bce		•		
	Windows Communication Foundation N	Windows Communication F	Bce	Фильтровать по группе	•		
	🜑 Беспроводные переносные устройства	Беспроводные переносны	Bce	Вид	•		
	🜑 Беспроводные переносные устройства	Беспроводные переносны	Bce	О Обновить			
	🥘 Дистанционное управление рабочим с	Дистанционное управлени	Bce				
	🥘 Домашняя группа: входящий трафик	Домашняя группа	Частныі	Экспортировать список			
	🔮 Домашняя группа: входящий трафик (Домашняя группа	Частныі	🛿 Справка			
	Журналы и оповещения производител	Журналы и оповещения п	Частныі				
	Журналы и оповещения производител	Журналы и оповещения п	Домен				
	Журналы и оповещения производител	Журналы и оповещения п	Домен				
	Журналы и оповещения производител	Журналы и оповещения п	Частныі				
	Инструментарий управления Windows	Инструментарий управлен	Частныі				
	Инструментарий управления Windows	Инструментарий управлен	Домен				
	Whcтрументарий управления Windows	Инструментарий управлен	Домен				
	Инструментарий управления Windows	Инструментарий управлен	Частныі				
	WHструментарий управления Windows	Инструментарий управлен	Частны				
	Инструментарий управления Windows	Инструментарий управлен	Домен				
	Инфраструктура одноранговых подкл	Инфраструктура одноранг	BCE				
	Инфраструктура одноранговых подкл	Инфраструктура одноранг	BCE				
	Инфраструктура одноранговых подкл	Инфраструктура одноранг	BCE				
	инфраструктура одноранговых подкл	инфраструктура одноранг	Бсе				
	Сординатор распределенных транзак	Координатор распределен	Домен				
	Координатор распределенных транзак	Координатор распределен	Лонон				
	Координатор распределенных транзак	Координатор распределен	Цастини				
	Координатор распределенных транзак	Координатор распределен	Частный				
	Координатор распределенных транзак	Координатор распределен	Ломен				
		Ловушка SNMP	Ломен				
	Служба ловушек SNMP (UDP In)	Ловушка SNMP	Частныі –				
<	< III	story and order					
				1			

3. Откроется окно Мастера создания правила для нового подключения. В нём нужно указать тип правила — Настраиваемые и перейти к следующему шагу по кнопке Далее.

🔗 Мастер создания прави	Мастер создания правила для нового входящего подключения				
Тип правила Выберите тип правила бранд	дмауэра, которое требуется создать.				
Шаги: Тип правила Программа	Правило какого типа вы хотите создать?				
 Протокол и порты Область Действие 	 Для программы Правило, управляющее подключениями для программы. Для порта Правило, управляющее подключениями для порта ТСР или UDP. 				
 Профиль Имя 	 Предопределенные ВranchCache - обнаружение кзширующих узлов (использует WSD) Правило, управляющее подключениями для операций Windows. Настраиваемые Настраиваемое правило. 				
	<u>Подробнее о типах правил</u> < Назад Далее > Отмена				

4. В пунктах Программа и Протокол и порты не требуется менять установки по умолчанию.

🔗 Мастер создания правила	для нового входящего подключения	X					
Программа	Программа						
Укажите полный путь и имя ис	полняемого файла программы, которой соответствует данное правило.						
Шаги:							
🧉 Тип правила	Применять это правило ко всем программам или к определенной программе?						
🧼 Программа							
🧶 Протокол и порты	Все программы						
🧼 Область	правило применяется ко всем подключениям компьютера, отвечающим другим свойствам правила.						
Действие	🔘 Путь программы:						
Профиль	Обзор						
• Имя	Пример: c:\path\program.exe %ProgramFiles%\browser\browser.exe						
	Службы Настроить Укажите службы, к которым применяется правило.						
	Подробнее об указании программ < Назад Далее > Отме	на					

Мастер создания правила для нового входящего подключения					
Протокол и порты					
Укажите протоколы и порты, к которым применяется данное правило.					
Шаги:					
🧼 Тип правила	Укажите порты и прот	Укажите порты и протоколы, к которым применяется это правило.			
Программа					
Протокол и порты	Тип протокола:	Любой 👻			
🧶 Область	Номер протокола:				
Действие					
Профиль	Локальный порт:	Все порты 👻			
• Имя					
		Пример: 80, 443, 5000-5010			
	Удаленный порт:	Все порты			
		Пример: 80, 443, 5000-5010			
	Параметры протокола	а ІСМР: Настроить			
	<u>Дополнительные све</u>	аения о протоколах и портах			
		Спазад Далее У Отмена			
[

В разделе Область следует установить переключатель удаленные IP-адреса в положение Указанные и нажать на кнопку Добавить.

🔗 Мастер создания правила	а для нового входящего подключения	×
Область		
Укажите локальный и удаленн	ый IP-адреса, к которым применяется данное правило.	
Шаги:		
Тип правила		
Программа	Укажите локальные IP-адреса, к которым применяется данное правило.	
Протокол и порты	Окобой IP-адрес	
🧼 Область	Указанные IP-адреса:	
Действие	Добавить	
🧶 Профиль	Изменить	
🕘 Имя		
	Настройка типов интерфейсов, к которым применимо данное Настроить	
	Укажите удаленные IP-адреса, к которым применяется данное правило.	
	Любой IP-адрес	
	Указанные IP-адреса:	
	Добавить	
	Изменить	
	Vasuer	
	<u>дополнительные сведения оо указании ооластеи</u>	
	< Назад Далее > От	мена

5. В открывшемся окне, нужно указать адрес удалённой подсети и нажать ОК.

IP-адрес	×				
Укажит	те IP-адреса для соответствия:				
⊚ IP-a	адрес или подсеть:				
192	2.168.1.0/24				
Прі	Примеры: 192.168.0.12 192.168.1.0/24 2002:9d3b:1a31:4:208:74ff.fe39:6c43 2002:9d3b:1a31:4:208:74ff.fe39:0/112				
⊚ Диа	апазон IP-адресов:				
c:					
по:					
🔘 Зар	Заранее заданный набор компьютеров:				
Oci	Основной шлюз 👻				
<u>Дополнительные сведения об указании IP-адресов</u>					
	ОК Отмена				

В случае если правилом требуется разрешить доступ с компьютера в локальной сети VPNсервера (правило создаётся на компьютере в локальной сети клиента VPN), указывается подсеть на Домашнем интерфейсе сервера VPN.

Если правило создаётся на компьютере в локальной сети VPN-сервера (требуется для разрешения входящих подключений из сети за клиентом VPN), нужно указать подсеть, включающую адрес выданный клиенту от сервера (по умолчанию на интернет-центре это подсеть 172.16.1.0/24).

Можно указать несколько подсетей если к компьютеру требуется выполнять подключения из различных удалённых расположений. После ввода требуемых значений, в окне Мастера нужно нажать Далее.

Мастер создания правила для нового входящего подключения				
Область				
Укажите локальный и удаленны	ый IP-адреса, к которым применяется данное правило.			
Шаги:				
Тип правила				
Программа	Укажите локальные IP-адреса, к которым применяется данное правидо.			
Протокол и порты	Опоследние и последние и после Опоследние и последние и после Опоследние и последние и по Опоследние и последние и Опоследние и последние и после Опоследние и последние и после Последние и последние и после Последние и последние и после Последние и последние и по Последние и последние и после Последние и последние			
🥥 Область	Указанные IP-адреса:			
Действие	Добавить			
🥘 Профиль	Изменить			
• Имя				
	S ADINIO			
	Настройка типов интерфейсов, к которым применимо данное Настроить			
	Укажите удаленные IP-адреса, к которым применяется данное правило.			
	Любой IP-адрес			
	Указанные IP-адреса:			
	192.168.1.0/24 Добавить			
	Изменить			
	Удалить			
	Лополнительные сведения об указании областей			
	< Назад Далее > Отм	лена		

6. В следующем шаге, в разделе Действие оставим предустановленное значение Разрешить подключение и перейдём далее.

🔗 Мастер создания правила	для нового входящего подключения	×				
Действие						
Укажите действие, выполняем	Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.					
Шаги:						
🧼 Тип правила	Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.					
🧼 Программа	 Разрешить подключение 					
 Протокол и порты Область 	Включая как подключения, защищенные IPSec, так и подключения без защиты.					
 Действие 	Разрешить безопасное подключение					
• Профиль	Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в					
• Имя	разделе правил оезопасности подключении. Настроить					
	Блокировать подключение					
	Подробнее о действиях					
	< Назад Далее > Отме	на				

7. Раздел **Профиль** предоставляет возможность выбрать профиль, к которому будет относиться настроенное правило. Поскольку настройка выполняется для компьютера, подключенного в Домашней сети интернет-центра, достаточно оставить галочку напротив профиля **Частный**.

💣 Мастер создания правил	па для нового входящего подключения	×
Профиль Укажите профили, к которым	применяется это правило.	
Шаги:		
🧶 Тип правила	Для каких профилей применяется правило?	
Программа		
🧶 Протокол и порты	🔲 Доменный	
💩 Область	Применяется при подключении компьютера к домену своей организации.	
Действие	📝 Частный	
🕘 Профиль	Применяется при подключении компьютера к частной сети.	
🥚 Имя	🔲 Публичный	
	Подробнее о профилях	
	< Назад Далее > Отме	эна

8. На завершающем шаге настройки, требуется указать имя правила и можно добавить поясняющее описание. По нажатию кнопки **Готово** мастер завершает работу.

Имя Укажите имя и описание данно	го правила.
Шаги:	
🧿 Тип правила	
Программа	
Протокол и порты	
• Область	Имя:
Действие	Входящие_VPN
• Профиль	<u>О</u> писание (необязательно):
V 11/12	
	< Назад <u>Готово</u> Отмена

9. Теперь, в окне представления **Правила для входящих подключений** отображается созданное правило. В последних версиях Windows для применения настройки дополнительных действий не требуется.

🔐 Брандмауэр Windows в режиме повышенной безопасности					x
Файл Действие Вид Справка					
💣 Брандмауэр Windows в режим	Правила для входящих подключений			Действия	
🔣 Правила для входящих по,	Имя	Группа	Профил 🔦	Правила для входящих подключений	
Правила для исходящего г Правила безопасности по	🕑 Входящие_VPN		Частныі	🗽 Создать правило	
 Наблюдение 	🔘 Обнаружение кэширующих узлов Bran	BranchCache - обнаружен	Bce	Фильтровать по профилю	•
	Получение содержимого BranchCache	BranchCache - получение	Bce ≡		
	🜑 Сервер размещенного кэша BranchCa	BranchCache - сервер разм	Bce		
	Secure Socket Tunneling Protocol (SSTP	Secure Socket Tunneling Pr	Bce	Фильтровать по группе	•
	Windows Communication Foundation N	Windows Communication F	Bce	Вид	►
	Беспроводные переносные устройства	Беспроводные переносны	Bce	о Обновить	
	Беспроводные переносные устройства	Беспроводные переносны	Bce		
	Дистанционное управление рабочим с	Дистанционное управлени	Bce		
	Одомашняя группа: входящий трафик	Домашняя группа	Частныі	👔 Справка	
	Домашняя группа: входящий трафик (Домашняя группа	Частны	Входящие VPN	
	Журналы и оповещения производител	Журналы и оповещения п	Частны		
	Журналы и оповещения производител	Журналы и оповещения п	Домен	Сполючить правило	
	С журналы и оповещения производител	журналы и оповещения п	Домен	🔏 Вырезать	
	Сурналы и оповещения производител	журналы и оповещения п Инструментарий управлен	Частный	🖹 Копировать	
	Инструментарий управления Windows	Инструментарии управлен	Ломен	🗙 Удалить	
	Инструментарий управления Windows	Инструментарии управлен	Ломен		
	Mucroymentapui управления Windows	Инструментарий управлен	Частныі		
	Mucroymentapui управления Windows	Инструментарий управлен	Частныі	👔 Справка	
	Инструментарий управления Windows	Инструментарий управлен	Домен		
	Инфраструктура одноранговых подкл	Инфраструктура одноранг	Bce		
	Инфраструктура одноранговых подкл	Инфраструктура одноранг	Bce		
	Мифраструктура одноранговых подкл	Инфраструктура одноранг	Bce		
	Инфраструктура одноранговых подкл	Инфраструктура одноранг	Bce		
	Координатор распределенных транзак	Координатор распределен	Домен		
	Координатор распределенных транзак	Координатор распределен	Частныі		
	🔘 Координатор распределенных транзак	Координатор распределен	Домен		
	🔘 Координатор распределенных транзак	Координатор распределен	Частныі		
	🔘 Координатор распределенных транзак	Координатор распределен	Частныі		
	🔘 Координатор распределенных транзак	Координатор распределен	Домен		
	🔘 Служба ловушек SNMP (UDP In)	Ловушка SNMP	Домен 👻		
۲ (III) (I	< III		•		

В случае если Windows-компьютер подключен к локальной сети ИЦ, являющегося VPNсервером и к нему требуется выполнять подключения из удалённой сети (за клиентом), в разрешающем правиле межсетевого экрана следует указать подсеть из которой выдаются адреса VPN-клиентам на сервере. По умолчанию на интернет-центрах Keenetic под управлением NDMS v2 адреса при подключении к VPN-серверу выдаются клиентам из подсети частного диапазона 172.16.1.0/24.

ZyXEL Keenetic Ultra			
Приложения			
Файл подкачки Сеть MS Windows FTP	Права доступа Клиент BitTorre	nt Cepsep DLNA	Сервер VPN
Сервер VPN (РРТР)			
Сервер VPN позволяет получить доступ к у вне дома. Подключения разрешены <u>польз</u> включить опцию "Транслировать адреса кл	истройствам вашей домашней сети <u>зователям системы</u> с правом дост пиентов (NAT)°	і с компьютеров и м упа "vpn". Для достуг	обильных устройств с подключением к интернету па клиентов VPN-сервера в Интернет необходимо
Включить:	<		
Одно подключение на пользователя:	✓		
Разрешить подключения без шифрования:			
Транслировать адреса клиентов (NAT):	✓		
Доступ к сети:	Home network (Wired and wireless	s hosts) (Home) 🗸	
Начальный адрес пула:	172.16.1.33		
Размер пула адресов:	10		
	Применить		
Имя пользователя	ІР-адрес	Д	оступ разрешен
admin	Нет	He	et
net_1	172.16.1.2	Да	3
alexander	Нет	Да	1

Если компьютер, к которому требуется установить удалённое подключение, расположен в сети интернет-центра, являющегося клиентом VPN, в разрешающем правиле файервола Windows потребуется указать подсеть адрес из которой установлен на интерфейсе подключающегося изза VPN-сервера компьютера. Согласно схеме <u>http://zyxel.ru/sites/default/files/kb/KB-4214/4214-01.jpg</u> в статье Б3-4214, это сеть 192.168.2.0/24.