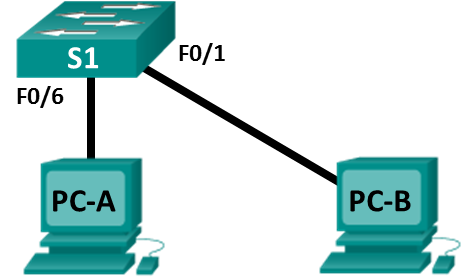
Лабораторная работа. Настройка параметров брандмауэра

1. Топология



1. Таблица адресации

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |
| PC-B | NIC | 192.168.1.11 | 255.255.255.0 |

1. Цели:

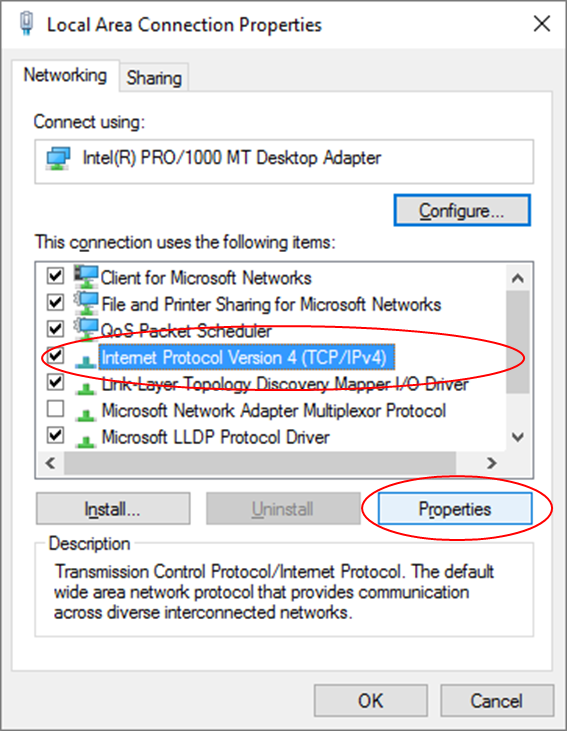
* доступ к настройкам брандмауэра Windows для добавления нового правила брандмауэра;
* создание правила брандмауэра для разрешения ping-запросов;
* удаление нового правила брандмауэра для возврата настроек в их прежнее состояние.

1. Исходные данные/сценарий

Если эхо-запросы с помощью команды ping с других компьютеров не проходят на ваш ПК, возможно, их блокирует брандмауэр. Многие из лабораторных работ предлагают вам выключить брандмауэр Windows для правильной обработки ping-запросов и ответов. Отключение брандмауэра не является рекомендуемой практикой в реальной производственной сети. В этой лабораторной работе вы создадите правило в брандмауэре для разрешения прохождения ping-запросов, не подвергая ПК другим типам атак, а также как отменить новое правило ICMP по завершении лабораторной работы.

1. Необходимые ресурсы:

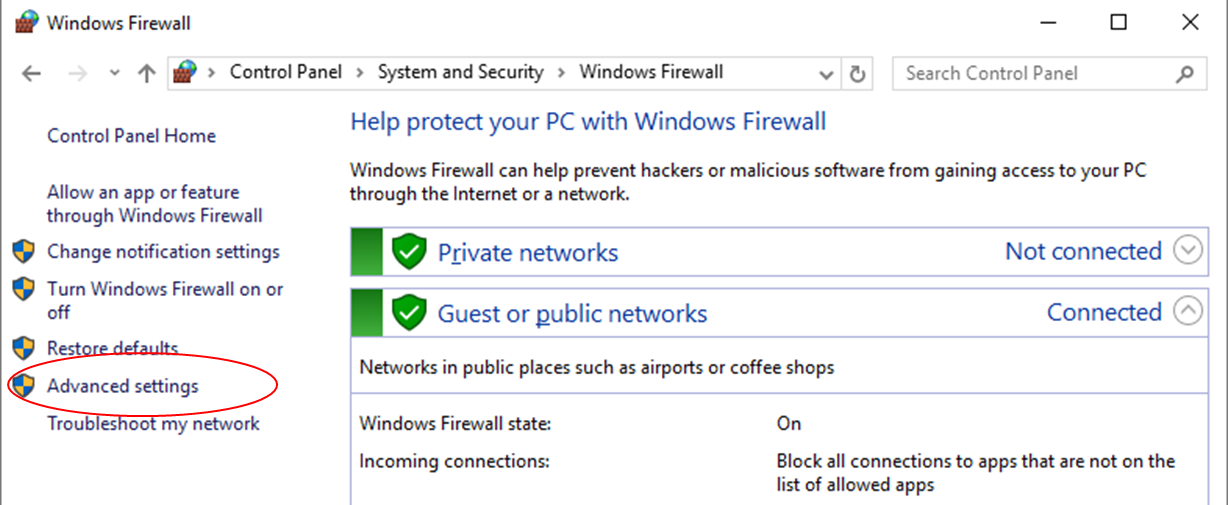
* 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель);
* 2 компьютера (Windows 10);
* 2 кабеля Ethernet, как показано в топологии.
  + 1. Проверьте, активен ли брандмауэр Windows и блокирует ли он ICMP-запросы.
       1. Щелкните правой кнопкой мыши **Пуск**. Выберите **Сетевые подключения**.
       2. Щелкните правой кнопкой мыши необходимый адаптер и выберите **Свойства**.
       3. Выберите **Протокол Интернета версии 4 (TCP/IPv4)**. Щелкните **Свойства** для настройки двух ПК с использованием статических IP-адресов, показанных в таблице адресации. В данной лабораторной работе нет необходимости в настройке основного шлюза или DNS-сервера, т. к. оба ПК находятся в одной IP-сети и будут использовать IP-адреса вместо доменных имен.



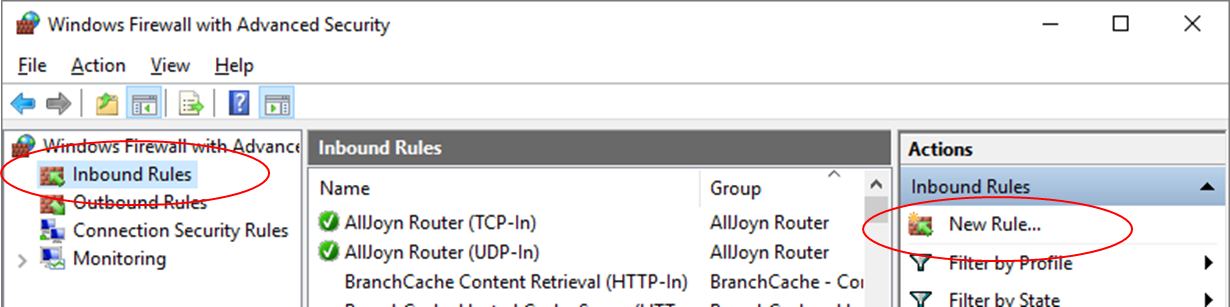
* + - 1. Откройте окно командной строки на ПК-A, щелкнув правой кнопкой мыши **Пуск** > **Командная строка**. Выполните команду **ping**, указав IP-адрес, назначенный для ПК-B. Команда **ping** должна вернуть отрицательный ответ. Повторите команду **ping** на ПК-B, выполните команду **ping**, указав IP-адрес, назначенный для ПК-A. Команды **ping** с обоих ПК должны вернуть отрицательный ответ, указывая на то, что брандмауэр Windows активен и блокирует ICMP-запросы.

**Примечание.** Если **ping-запрос** дает положительный отклик на каком-либо ПК, проверьте, активен ли брандмауэр Windows на обеих машинах.

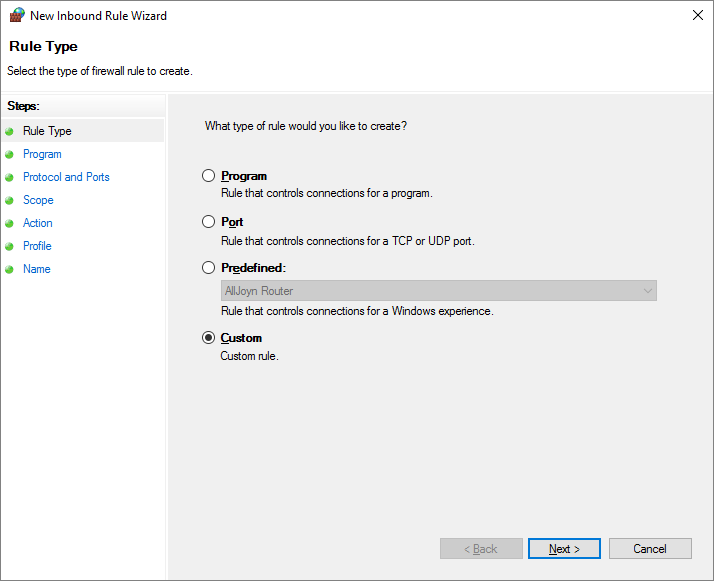
* + 1. Создайте новое правило, разрешающее прохождение ICMP-трафика через брандмауэр.
       1. Настройте параметры брандмауэра на ПК-А. Щелкните **Пуск** и введите **Брандмауэр**. Выберите **Брандмауэр Windows** в списке результатов.
       2. На левой панели окна брандмауэра Windows щелкните **Дополнительные параметры**.



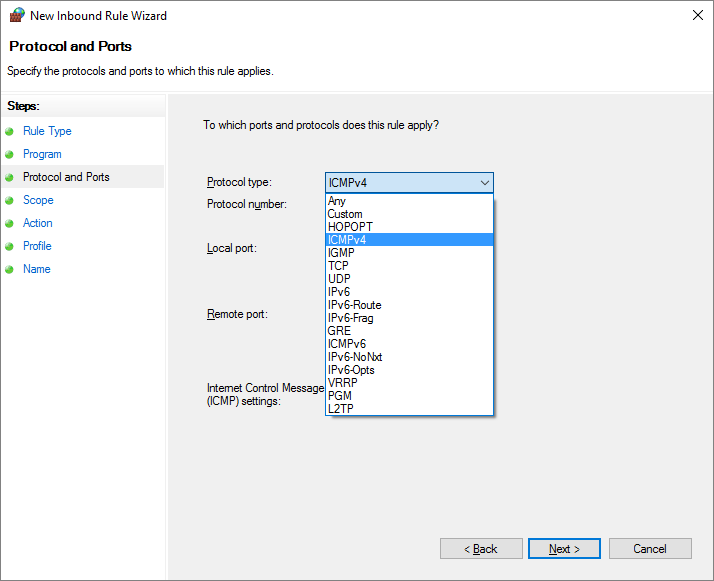
* + - 1. В окне «Дополнительные параметры безопасности» выберите параметр **Правила для входящих подключений** на левой боковой панели, а потом щелкните **Создать правило…** на правой боковой панели.



* + - 1. Нажатием пункта меню «Создать правило» открывается мастер создания правил для нового входящего подключения. На экране «Тип правила» щелкните переключатель **Настраиваемые** и нажмите **Далее**.



* + - 1. На левой панели щелкните параметр **Протокол и порты** и выберите **ICMPv4** из раскрывающегося меню «Тип протокола», затем щелкните **Далее**.

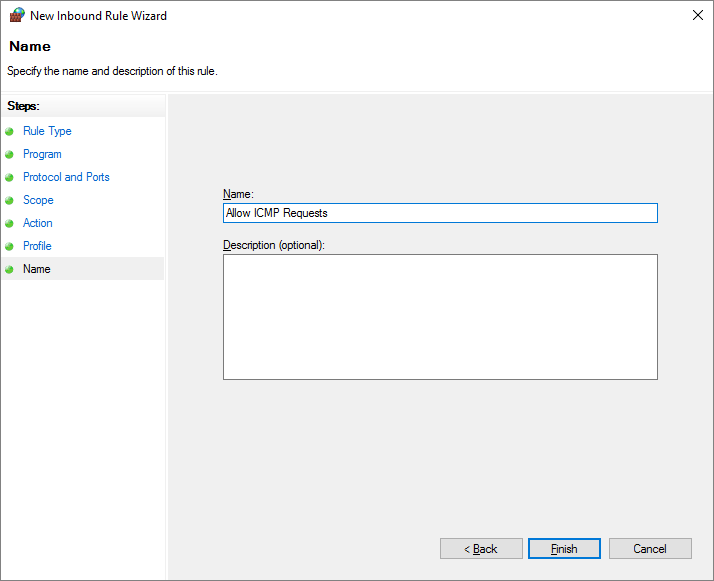


Составьте список из трех протоколов (в дополнение к ICMP), которые могут отфильтровываться новым правилом входящих подключений брандмауэра.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. На левой панели щелкните параметр **Имя** и в поле «Имя» введите **Разрешить запросы ICMP**. Щелкните **Finish (Готово)**.



Это новое правило позволит членам вашей команды получать ответы на **ping-запросы** от ПК-A. Повторите инструкции шага 2, чтобы добавить новое правило на ПК-B.

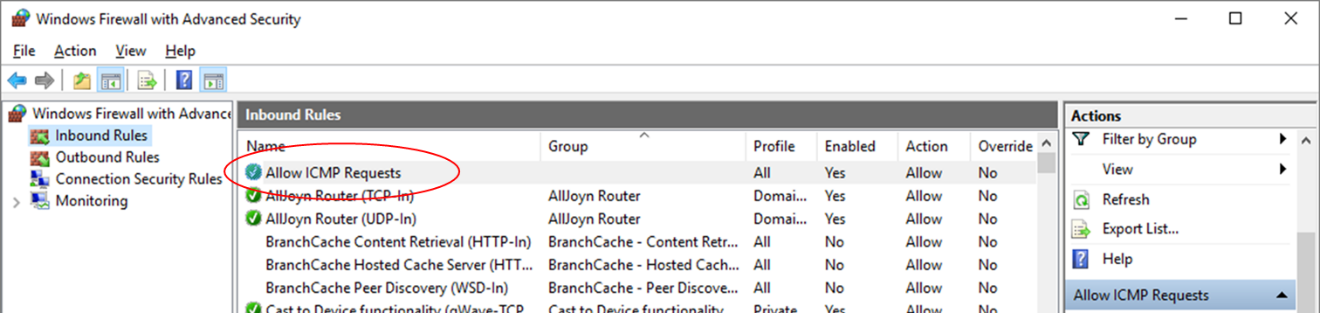
* + - 1. Проверьте новое правило брандмауэра путем повторного использования команд **ping,** использованных на шаге 1. Эти ping-запросы должны дать положительный отклик.

Если это не так, проверьте параметры брандмауэра, чтобы убедиться, что новое правило настроено корректно.

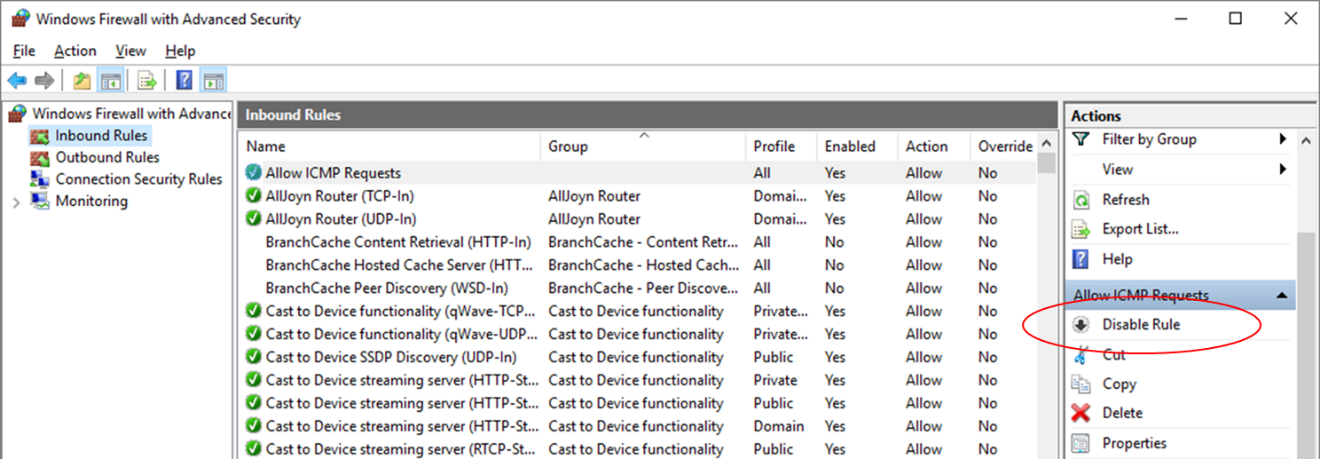
* + 1. Отключите и удалите новое правило ICMP.

По завершении лабораторной работы необходимо отключить или удалить новое правило, созданное в шаге 2. Использование параметра **Отключить правило** позволяет снова включить правило позже. Полное удаление правила навсегда удалит его из списка правил для входящих подключений.

* + - 1. В окне «Расширенные функции безопасности» на левой панели щелкните **«Правила для входящих подключений»**, а потом найдите правило, созданное на шаге 1.



* + - 1. Для отключения правила щелкните параметр **«Отключить правило»**. После этого она изменится на вариант **Включить правило**. Правило можно включать и отключать поочередно. Состояние правила также отображается в столбце «Включено» списка правил для входящих подключений.



* + - 1. Чтобы удалить правило ICMP навсегда, нажмите **Удалить**. Если после этого потребуется разрешить запросы ICMP, правило нужно будет создать заново.
      2. Выполните команды **ping,** выполненные на шаге 1, чтобы убедиться, что брандмауэр теперь снова блокирует запросы ping.