Лабораторная работа. Настройка параметров брандмауэра

Топология

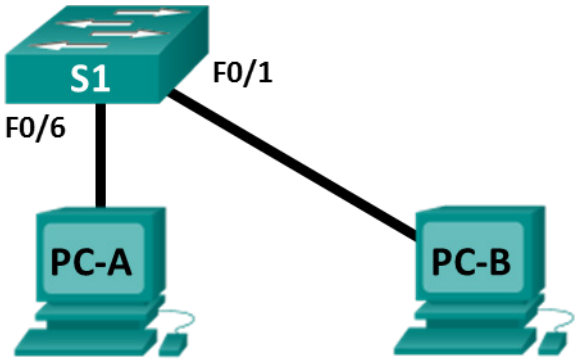


Таблица адресации

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

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.

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.

Необходимые ресурсы:

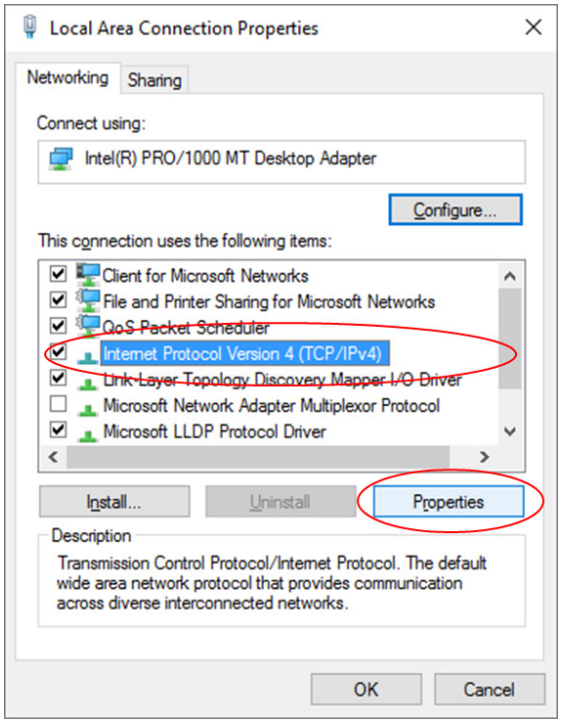
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель);
- 2 компьютера (Windows 10);
- 2 кабеля Ethernet, как показано в топологии.

Шаг 1: Проверьте, активен ли брандмауэр Windows и блокирует ли он ICMP-запросы.

a. Щелкните правой кнопкой мыши **Пуск**. Выберите **Сетевые подключения**.

b. Щелкните правой кнопкой мыши необходимый адаптер и выберите **Свойства**.

c. 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.



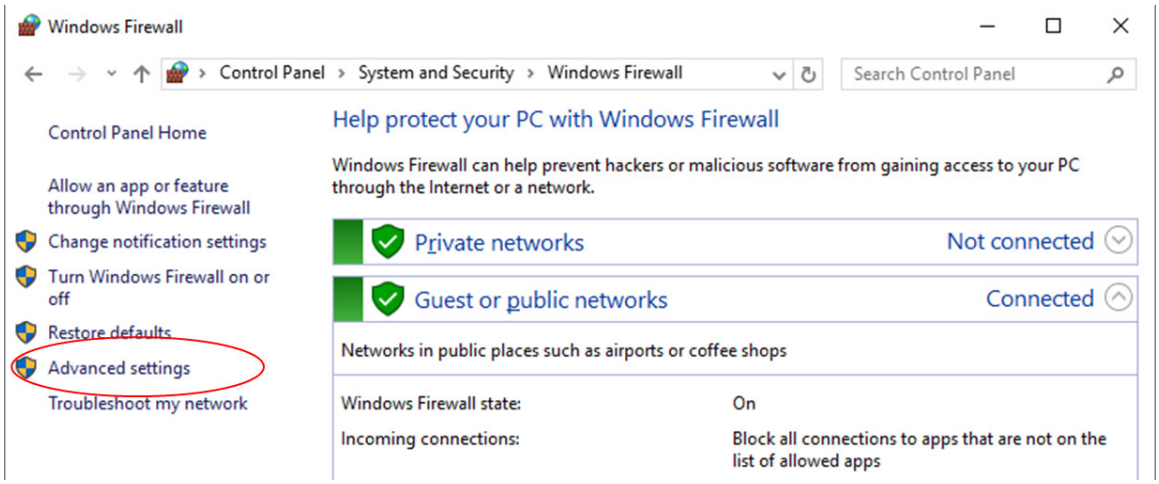
d. Откройте окно командной строки на ПК-A, щелкнув правой кнопкой мыши **Пуск** > **Командная строка**. Выполните команду **ping**, указав IP-адрес, назначенный для ПК-B. Команда **ping** должна вернуть отрицательный ответ. Повторите команду **ping** на ПК-B, выполните команду **ping**, указав IP-адрес, 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.

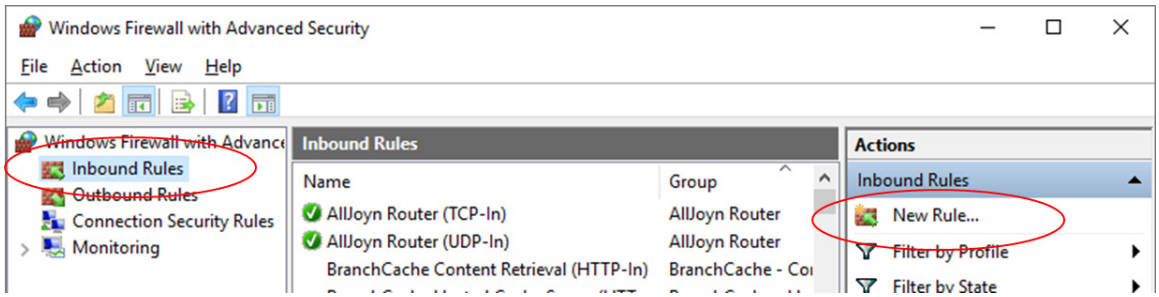
Шаг 2: Создайте новое правило, разрешающее прохождение ICMP-трафика через брандмауэр.

a. Настройте параметры брандмауэра на ПК-A. Щелкните **Пуск** и введите **Брандмауэр**. Выберите **Брандмауэр Windows** в списке результатов.

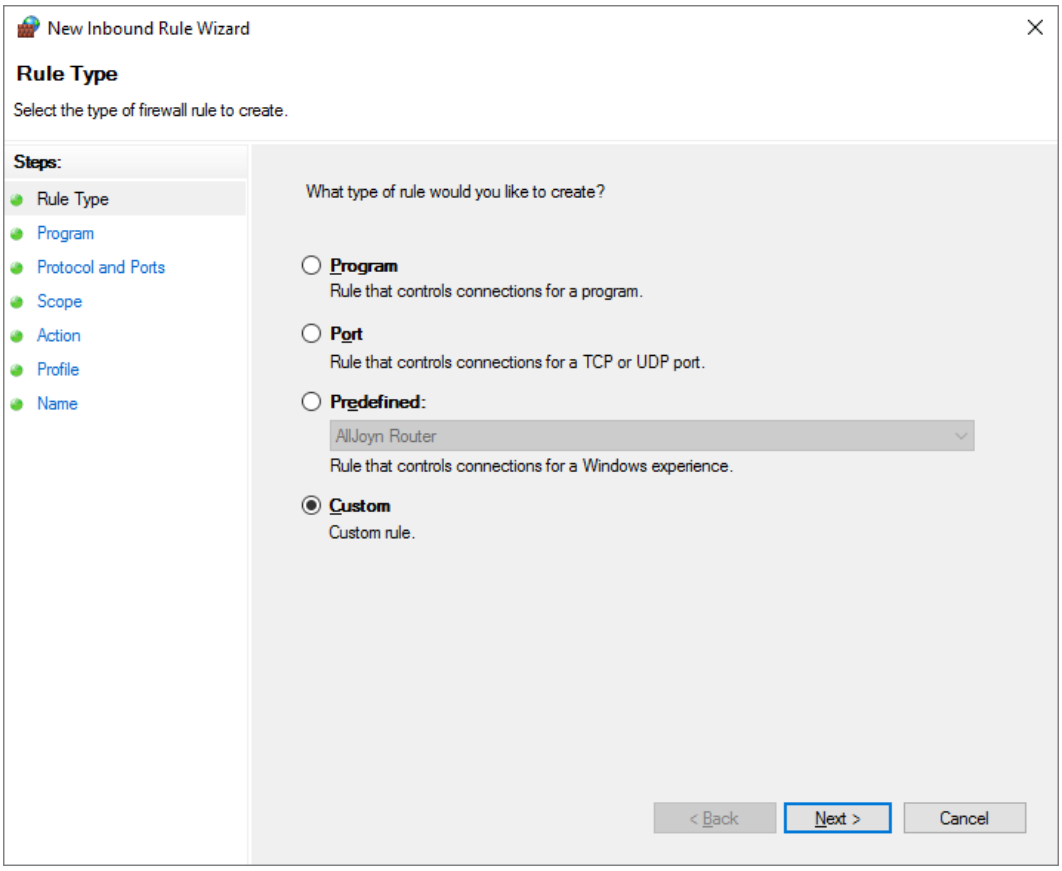
b. На левой панели окна брандмауэра Windows щелкните **Дополнительные параметры**.



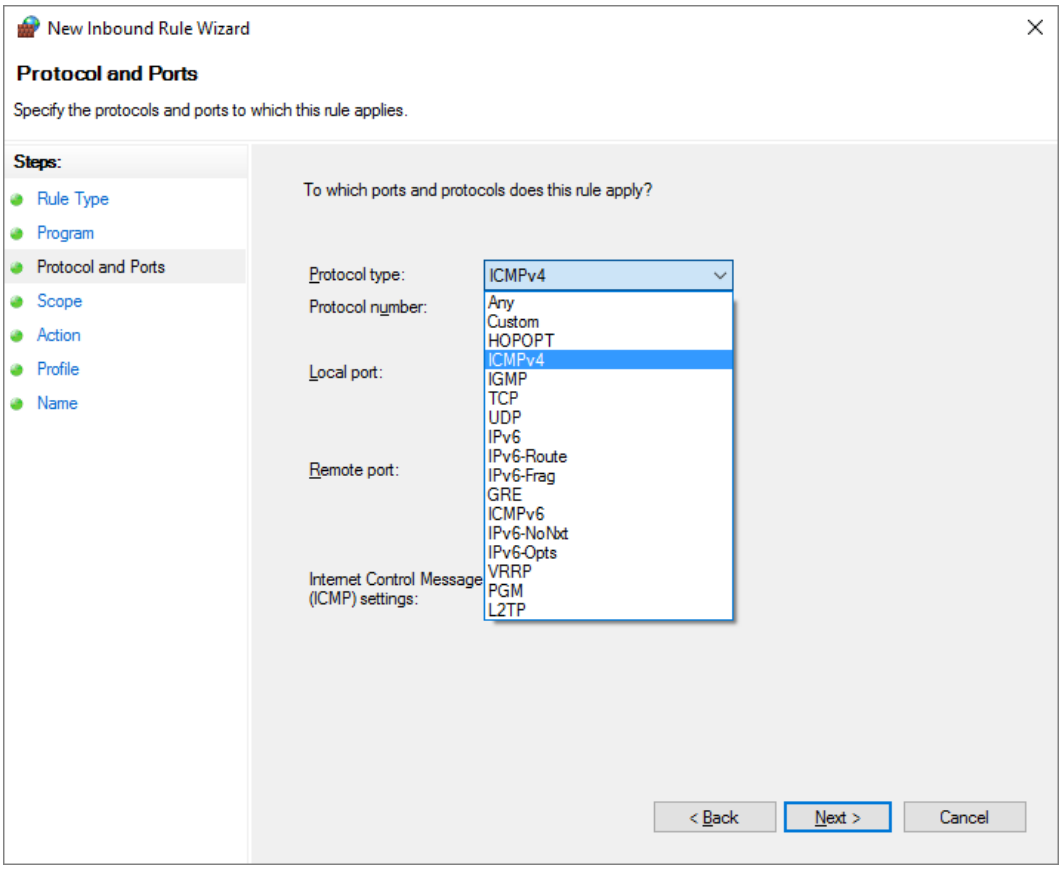
c. В окне «Дополнительные параметры безопасности» выберите параметр **Правила для входящих подключений** на левой боковой панели, а потом щелкните **Создать правило…** на правой боковой панели.



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



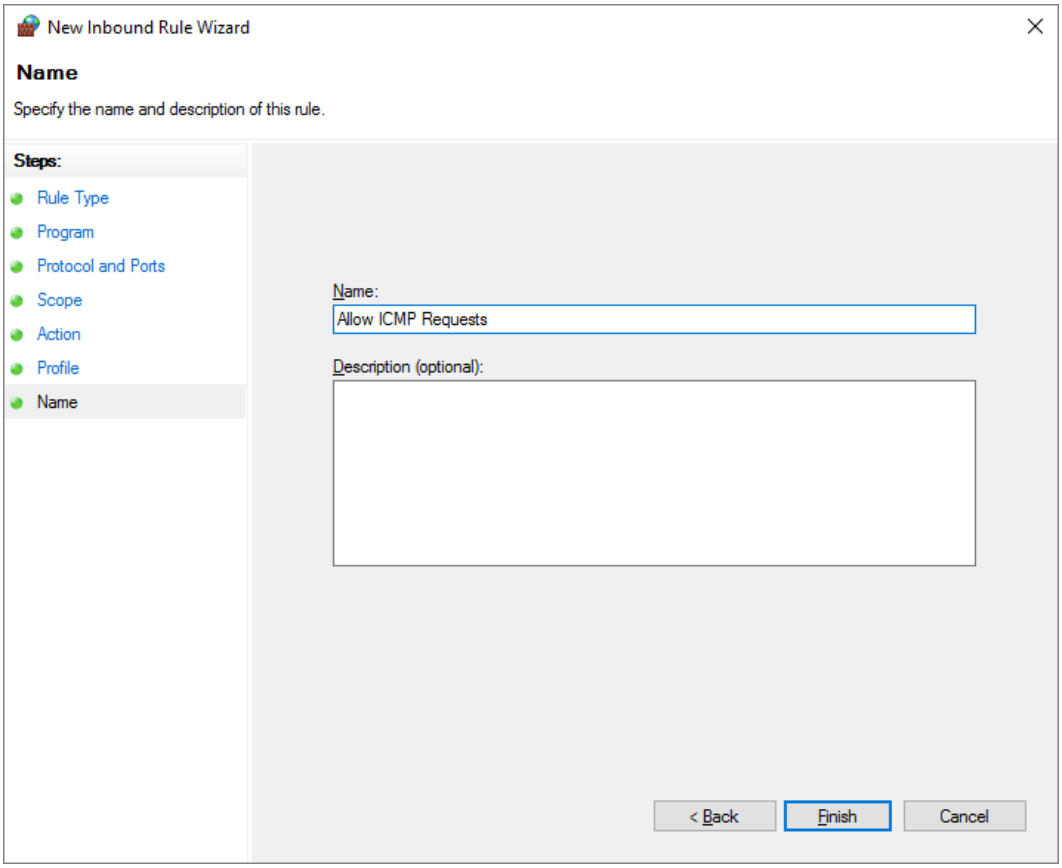
e. На левой панели щелкните параметр **Протокол и порты** и выберите **ICMPv4** из раскрывающегося меню «Тип протокола», затем щелкните **Далее**.



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

TCP; UDP; IGMP

f. 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-А. Повторите инструкции шага 2, чтобы добавить новое правило на ПК-В.

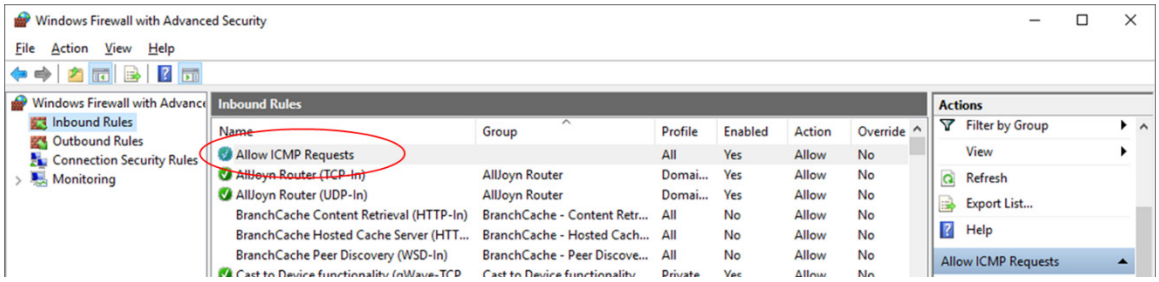
g. Проверьте новое правило брандмауэра путем повторного использования команд **ping,** использованных на шаге 1. Эти ping-запросы должны дать положительный отклик.

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

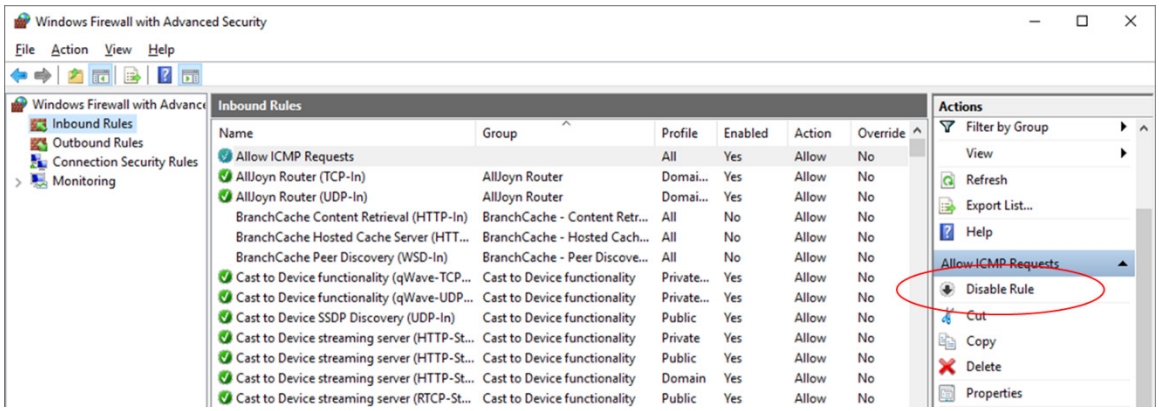
Шаг 3: Отключите и удалите новое правило ICMP.

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.

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



b. 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.



c. Чтобы удалить правило ICMP навсегда, нажмите **Удалить**. Если после этого потребуется разрешить запросы ICMP, правило нужно будет создать заново.

d. Выполните команды **ping,** выполненные на шаге 1, чтобы убедиться, что брандмауэр теперь снова блокирует запросы ping.