Лабораторная работа №7. Настройка межсетевого экрана в ОС Debian

Для проведения лабораторных работ будет использована схема сети, представленная на рисунке

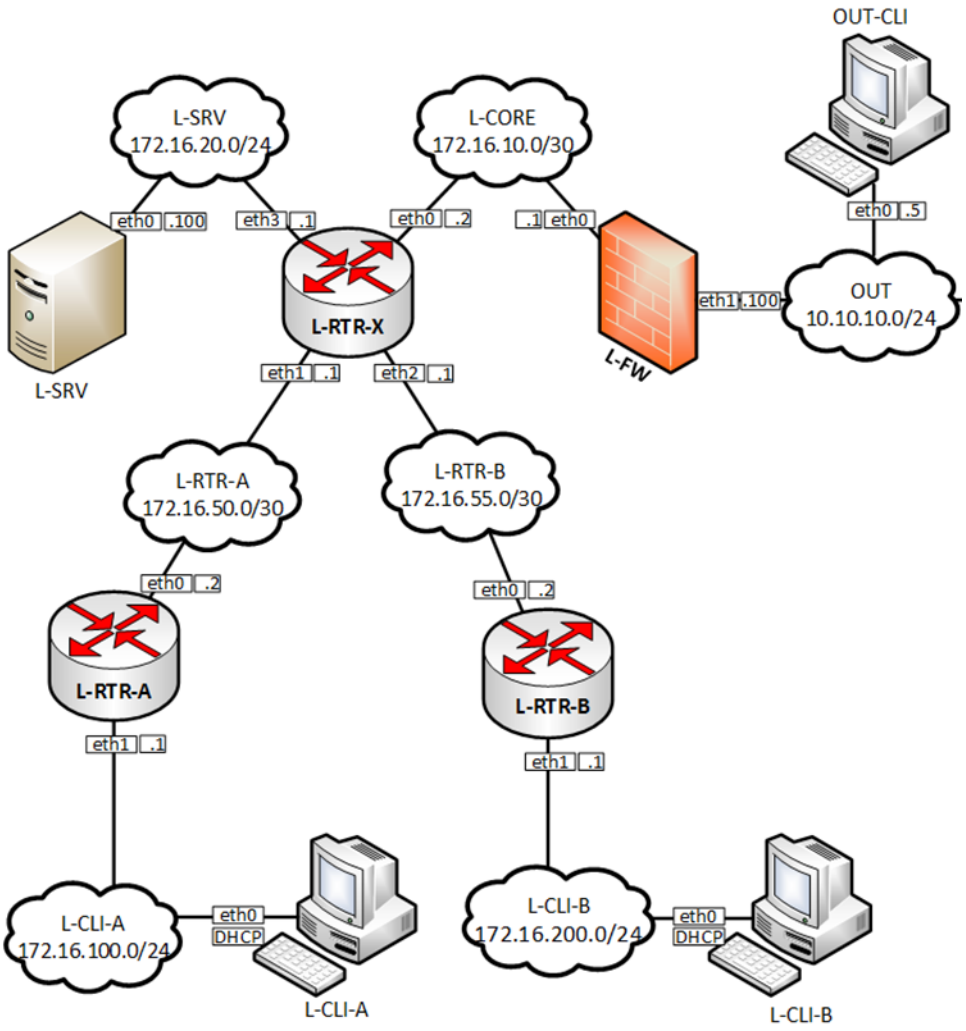


Рисунок 1. Топология сети

Схема сети содержит 8 виртуальных машин, выполняющих различные роли: L-RTR-X, L-RTR-A, L-RTR-B выполняют роли промежуточных сетевых устройств – маршрутизаторов, L-SRV, L-FW выполняют роль оконечных устройств – серверов, L-CLI-A, L-CLI-B, OUT-CLI выполняют роль рабочих станций пользователей. Все виртуальные машины работают под управлением ОС Debian.

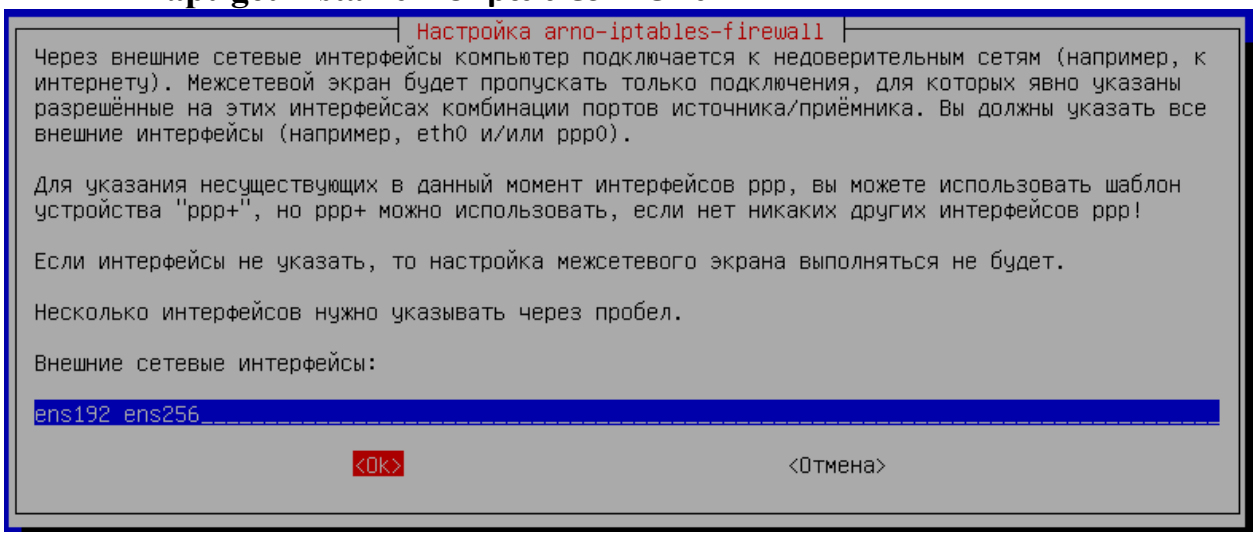
Настройка межсетевого экрана с помощью утилиты

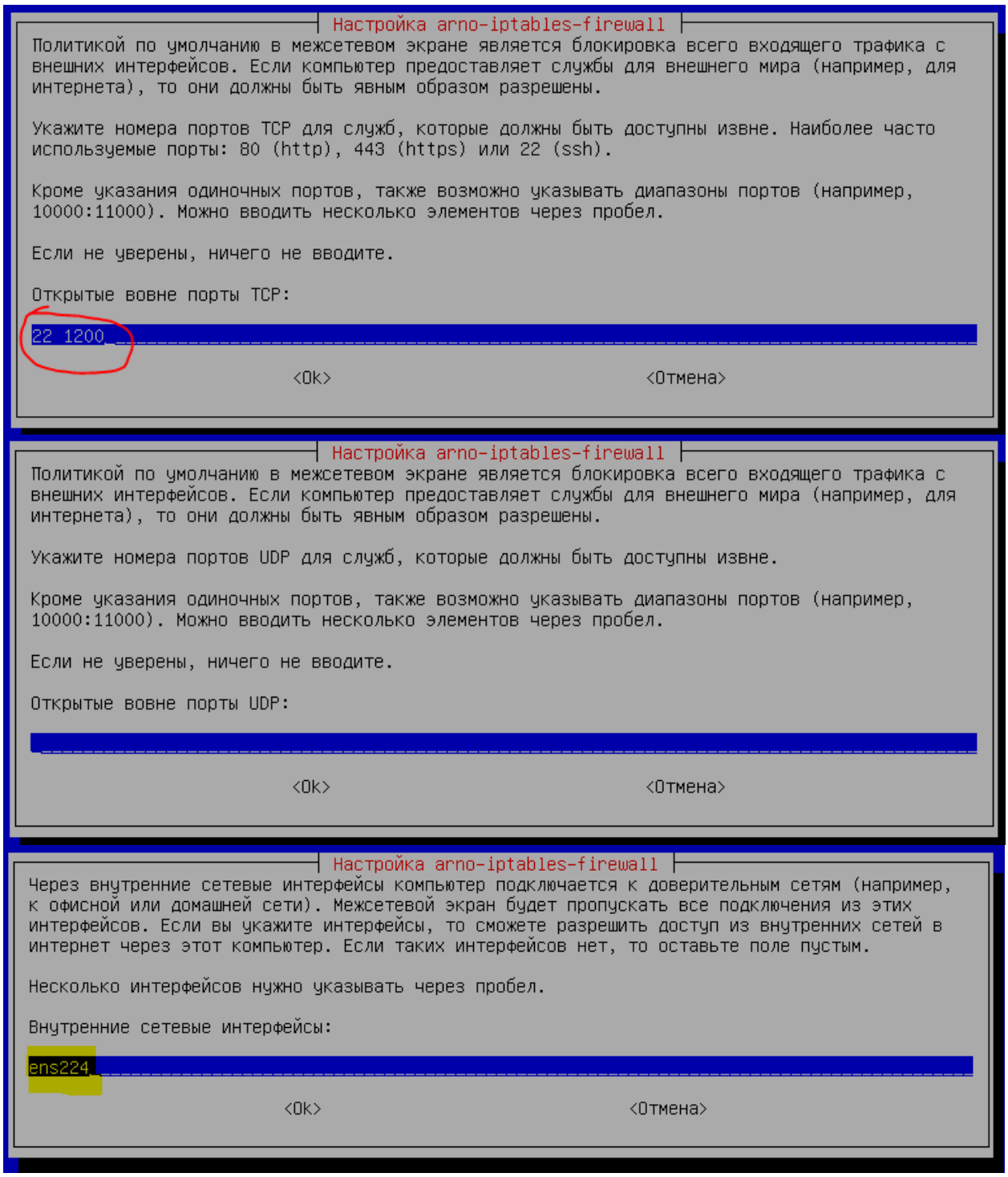
1) Межсетевой экран устанавливается на **L-FW**
2) На L-FW необходимо добавить дополнительный сетевой адаптер, который должен быть подключен к сети Интернет. Для этого адаптер должен быть включен в группу портов VM Network. Пусть его имя будет **ens256.** Сетевой адрес этот интерфейс должен получать автоматически от **внешнего сервера DHCP**. Либо настроить статический адрес. **Уточнить у преподавателя!!!**
3) Проверяем наличие **iptables** в системе:
   `#dpkg -l | grep iptables`
   и если его нет, то устанавливаем
   #apt-get install iptables

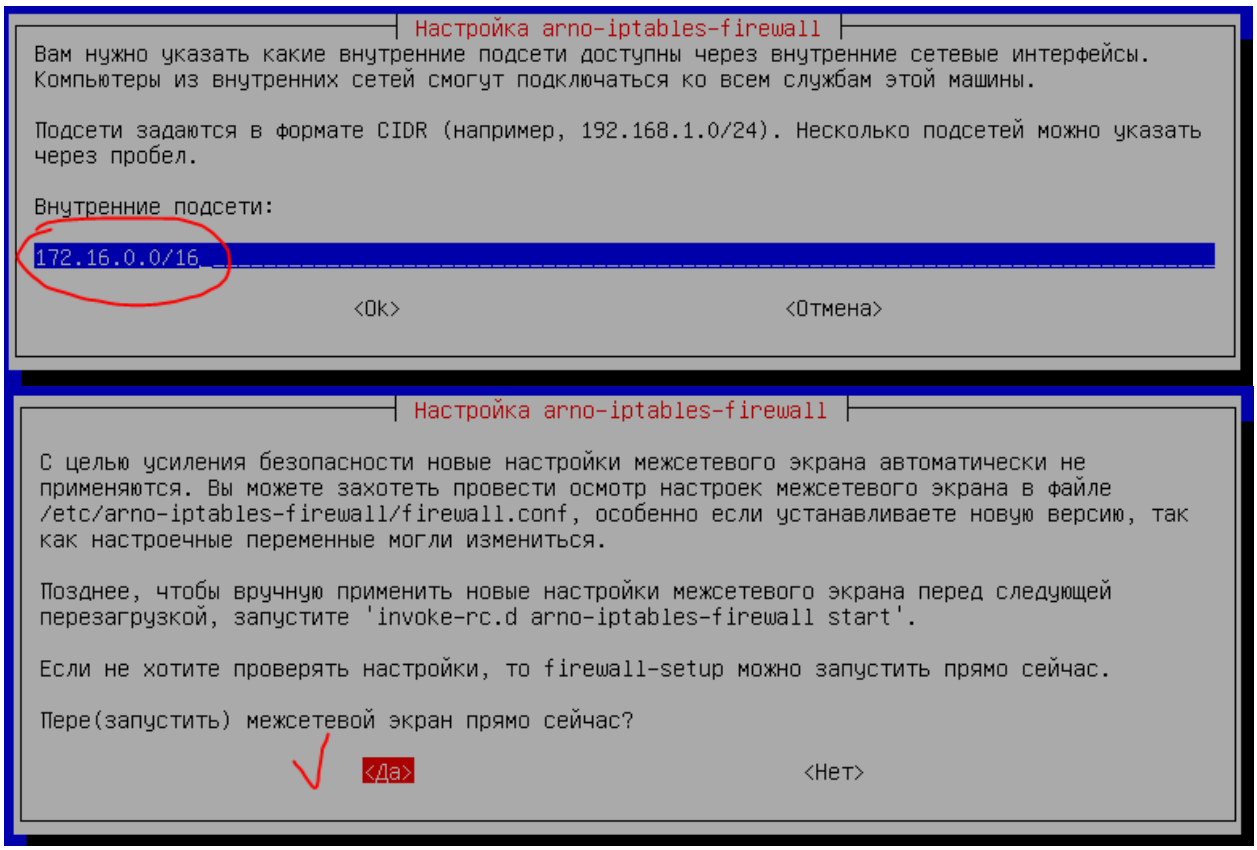
4) Добавить в список источников **/etc/apt/sources.list** новый источник пакетов. **Добавлять, если не добавлен ранее**

   deb http://ftp.ru.debian.org/debian stretch main

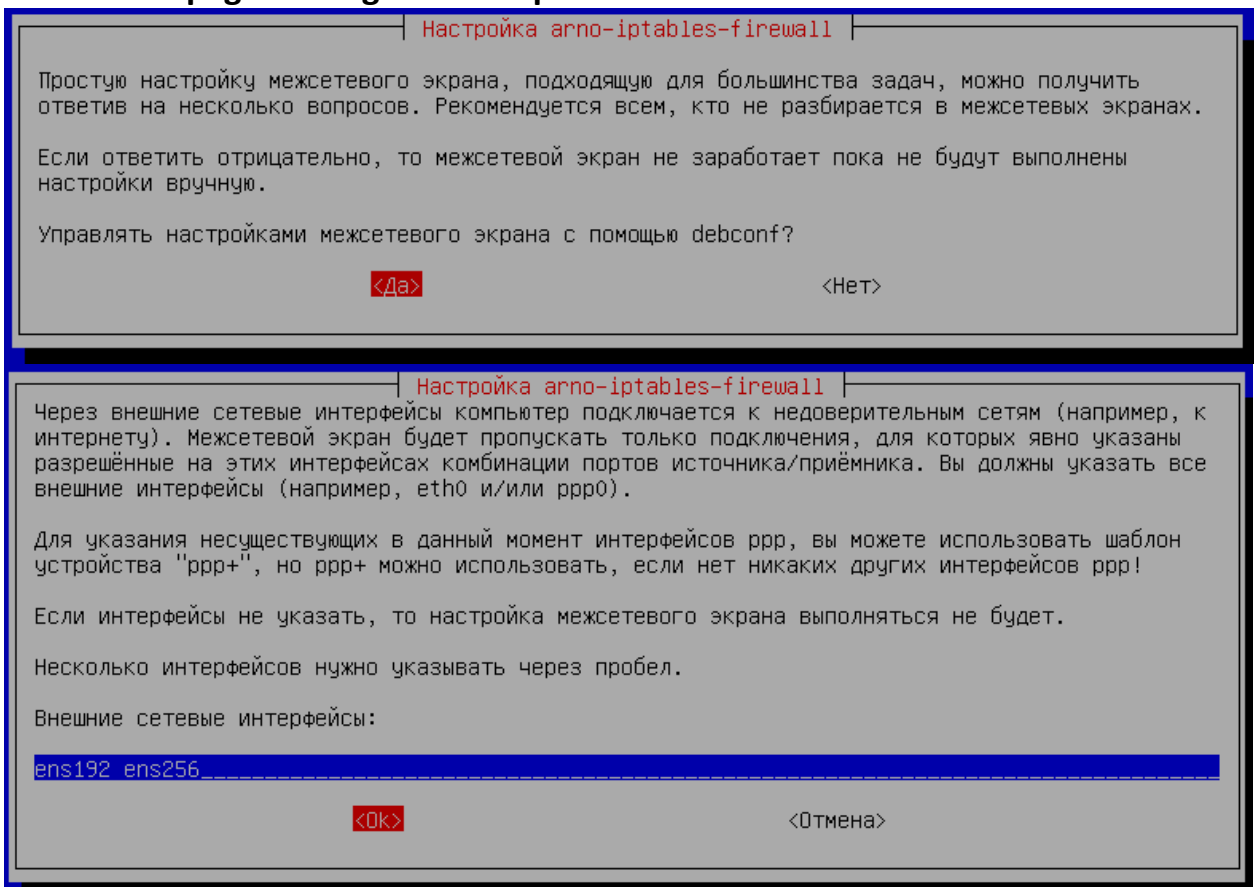
5) обновить локальный индекс пакетов до последних изменений в репозиториях:
   # apt-get update
6) установить пакет **arno-iptables-firewall**
   #apt-get install arno-iptables-firewall

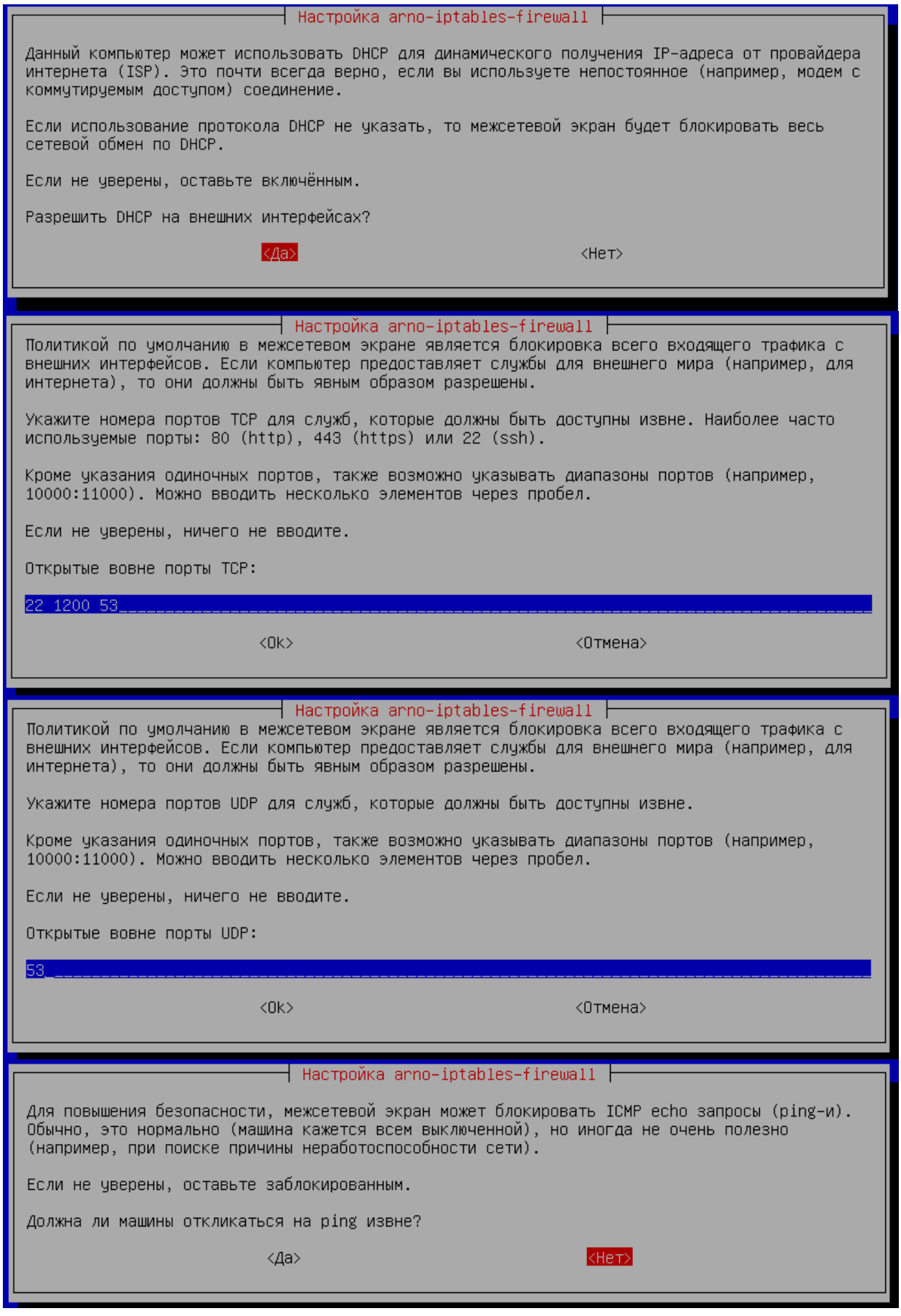


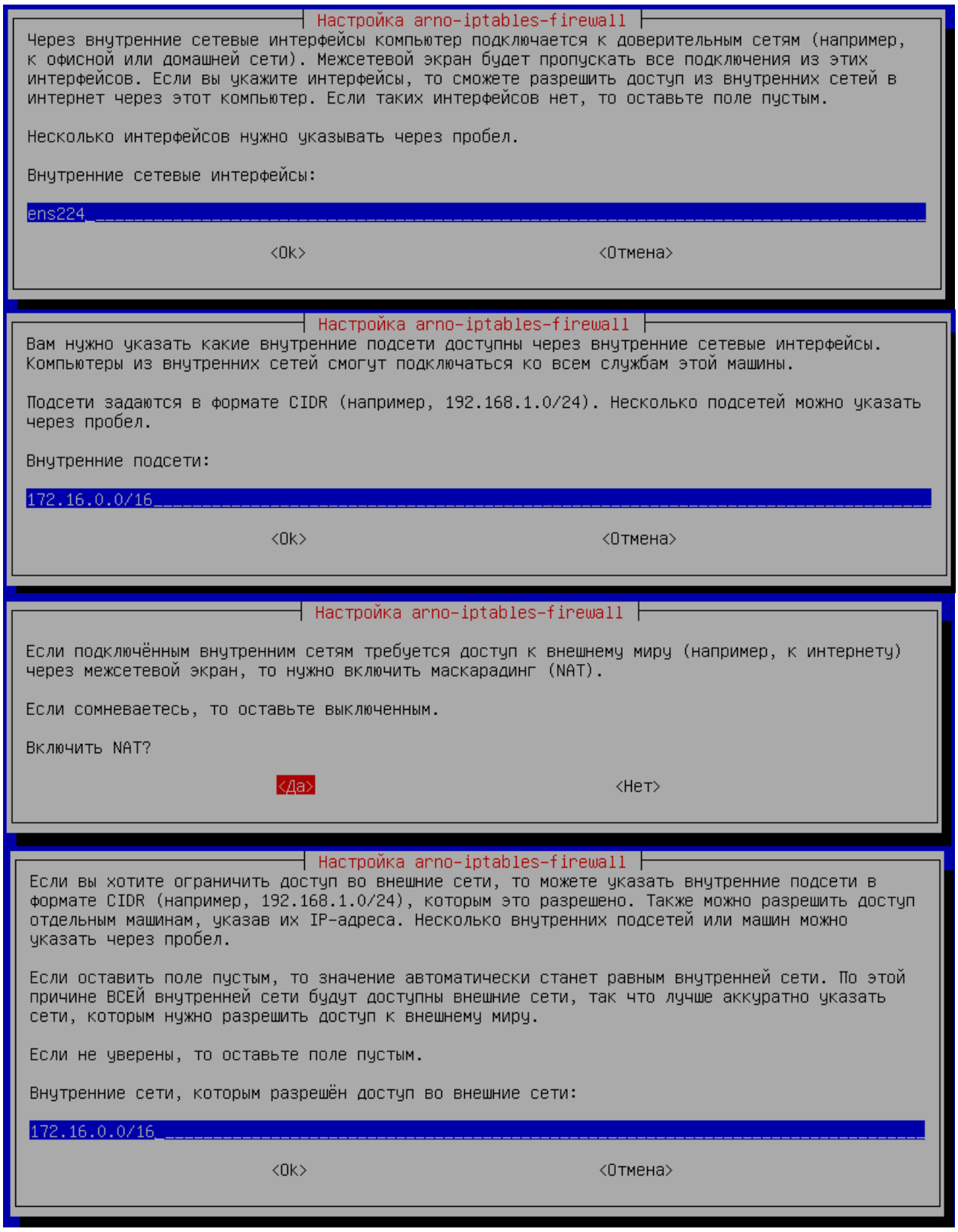

Настройка arno-iptables-firewall
Политикой по умолчанию в межсетевом экране является блокировка всего входящего трафика с внешних интерфейсов. Если компьютер предоставляет службы для внешнего мира (например, для интернета), то они должны быть явным образом разрешены.
Укажите номера портов TCP для служб, которые должны быть доступны извне. Наиболее часто используемые порты: 80 (http), 443 (https) или 22 (ssh).
Кроме указания одиночных портов, также возможно указывать диапазоны портов (например, 10000:11000). Можно вводить несколько элементов через пробел.
Если не уверены, ничего не вводите.
Открытые вовне порты TCP:
22 1200
<Ok>
<Отмена>
Настройка arno-iptables-firewall
Политикой по умолчанию в межсетевом экране является блокировка всего входящего трафика с внешних интерфейсов. Если компьютер предоставляет службы для внешнего мира (например, для интернета), то они должны быть явным образом разрешены.
Укажите номера портов UDP для служб, которые должны быть доступны извне.
Кроме указания одиночных портов, также возможно указывать диапазоны портов (например, 10000:11000). Можно вводить несколько элементов через пробел.
Если не уверены, ничего не вводите.
Открытые вовне порты UDP:
<Ok>
<Отмена>
Настройка arno-iptables-firewall
Через внутренние сетевые интерфейсы компьютер подключается к доверительным сетям (например, к офисной или домашней сети). Межсетевой экран будет пропускать все подключения из этих интерфейсов. Если вы укажите интерфейсы, то сможете разрешить доступ из внутренних сетей в интернет через этот компьютер. Если таких интерфейсов нет, то оставьте поле пустым.
Несколько интерфейсов нужно указывать через пробел.
Внутренние сетевые интерфейсы:
ens224
<Ok>
<Отмена>

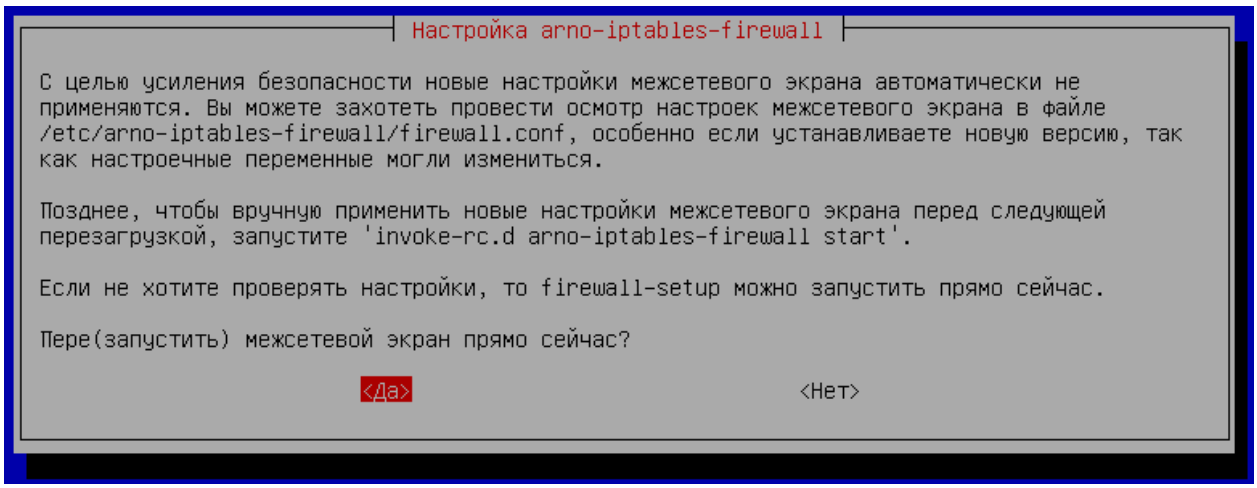


7) Работа с мастером
#dpkg-reconfigure arno-iptables-firewall




Настройка arno-iptables-firewall
Данный компьютер может использовать DHCP для динамического получения IP-адреса от провайдера интернета (ISP). Это почти всегда верно, если вы используете непостоянное (например, модем с коммутируемым доступом) соединение.
Если использование протокола DHCP не указать, то межсетевой экран будет блокировать весь сетевой обмен по DHCP.
Если не уверены, оставьте включённым.
Разрешить DHCP на внешних интерфейсах?
<Да>
<Нет>
Настройка arno-iptables-firewall
Политикой по умолчанию в межсетевом экране является блокировка всего входящего трафика с внешних интерфейсов. Если компьютер предоставляет службы для внешнего мира (например, для интернета), то они должны быть явным образом разрешены.
Укажите номера портов TCP для служб, которые должны быть доступны извне. Наиболее часто используемые порты: 80 (http), 443 (https) или 22 (ssh).
Кроме указания одиночных портов, также возможно указывать диапазоны портов (например, 10000:11000). Можно вводить несколько элементов через пробел.
Если не уверены, ничего не вводите.
Открытые вовне порты TCP:
22 1200 53
<Ok>
<Отмена>
Настройка arno-iptables-firewall
Политикой по умолчанию в межсетевом экране является блокировка всего входящего трафика с внешних интерфейсов. Если компьютер предоставляет службы для внешнего мира (например, для интернета), то они должны быть явным образом разрешены.
Укажите номера портов UDP для служб, которые должны быть доступны извне.
Кроме указания одиночных портов, также возможно указывать диапазоны портов (например, 10000:11000). Можно вводить несколько элементов через пробел.
Если не уверены, ничего не вводите.
Открытые вовне порты UDP:
53
<Ok>
<Отмена>
Настройка arno-iptables-firewall
Для повышения безопасности, межсетевой экран может блокировать ICMP echo запросы (ping-и). Обычно, это нормально (машина кажется всем выключенной), но иногда не очень полезно (например, при поиске причины неработоспособности сети).
Если не уверены, оставьте заблокированным.
Должна ли машины откликаться на ping извне?
<Да>
<Нет>


Настройка arno-iptables-firewall
Через внутренние сетевые интерфейсы компьютер подключается к доверительным сетям (например, к офисной или домашней сети). Межсетевой экран будет пропускать все подключения из этих интерфейсов. Если вы укажите интерфейсы, то сможете разрешить доступ из внутренних сетей в интернет через этот компьютер. Если таких интерфейсов нет, то оставьте поле пустым.
Несколько интерфейсов нужно указывать через пробел.
Внутренние сетевые интерфейсы:
ens224
<Ok>
<Отмена>
Настройка arno-iptables-firewall
Вам нужно указать какие внутренние подсети доступны через внутренние сетевые интерфейсы. Компьютеры из внутренних сетей смогут подключаться ко всем службам этой машины.
Подсети задаются в формате CIDR (например, 192.168.1.0/24). Несколько подсетей можно указать через пробел.
Внутренние подсети:
172.16.0.0/16
<Ok>
<Отмена>
Настройка arno-iptables-firewall
Если подключённым внутренним сетям требуется доступ к внешнему миру (например, к интернету) через межсетевой экран, то нужно включить маскарадинг (NAT).
Если сомневаетесь, то оставьте выключенным.
Включить NAT?
<Да>
<Нет>
Настройка arno-iptables-firewall
Если вы хотите ограничить доступ во внешние сети, то можете указать внутренние подсети в формате CIDR (например, 192.168.1.0/24), которым это разрешено. Также можно разрешить доступ отдельным машинам, указав их IP-адреса. Несколько внутренних подсетей или машин можно указать через пробел.
Если оставить поле пустым, то значение автоматически станет равным внутренней сети. По этой причине ВСЕЙ внутренней сети будут доступны внешние сети, так что лучше аккуратно указать сети, которым нужно разрешить доступ к внешнему миру.
Если не уверены, то оставьте поле пустым.
Внутренние сети, которым разрешён доступ во внешние сети:
172.16.0.0/16
<Ok>
<Отмена>



8) Добавить правило для iptables для разрешения трафика VPN
   # iptables –I FORWARD –s 10.2.2.0/24 –j ACCEPT

9) Сохранить настройки iptables в файл **iptables.default**

   #mkdir /etc/iptables
   #touch /etc/iptables/iptables.default
   #iptables-save > /etc/iptables/iptables.default

10) Обеспечить автоматическую загрузку правил при запуске сервера. Для этого необходимо добавить в файл **/etc/network/interfaces** одну строчку в секцию к внешнему интерфейсу (например, ens192).

    auto ens192
    iface ens192 inet dhcp
    post-up /sbin/iptables-restore < /etc/iptables/iptables.default

11) Сохранить файл **/etc/network/interfaces**

[redacted]

13) Посмотреть статус службы
    #systemctl status arno-iptables-firewall

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Установить и настроить межсетевой экран. Проверить работу межсетевого экрана с помощью проверки доступности внешних ip адресов