«Раздать доступ к интернет в локальной сети»

SuSe Linux 10.0
конфигурирование трансляции адресов (NAT)
с помощью «YaSt2».
«в картинках»

Версия документа 2006.11.15_0514

1. Цель: обеспечить «прозрачный» доступ к сети интернет с компьютеров расположенных в локальной сети с наименьшими затратами.

2. Условия :

Читатель должен: быть знаком с основами сетевых технологий (*иметь представление о том что такое «ip-адрес», «шлюз по умолчанию», «dns-сервер»*); быть способным настроить сетевой интерфейс (*назначить ip-адрес, шлюз, указать dns-сервера*).

В данном документе процесс настройки сетевых интерфейсов не рассматривается, обратитесь к другим руководствам.

На **компьютер**е который вы планируете использовать в качестве шлюза, должно быть корректно настроено два сетевых интерфейса, один – во внешнюю сеть, второй – во внутреннюю.

В дальнейшем этот компьютер именуется «сервером», компьютеры локальной сети на которых необходим доступ к «внешней сети» - «клиентами»

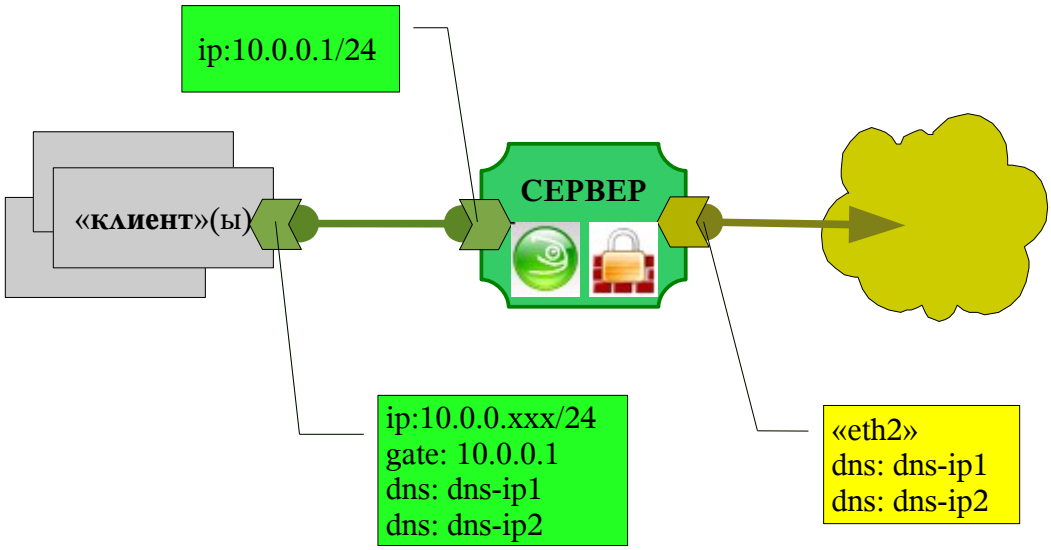
На этом компьютере установлен SuSe Linux (10.0 (и выше?)) и работает «SuSe Firewall».

Данное руководство проверялось на «не-динамических» интерфейсах (с назначением ip по dhcp). Работа с интерфейсами вида «ppp0», «bnep0» и др. автором не проверялась, хотя есть источники по которым можно судить что «все работает». (см раздел ссылки)

Документ «раздается как есть».Вы применяете рецепты описанные здесь на свой страх и риск. Претензии не принимаются, пожелания выслушиваются.

3. Что имеем.

Давайте сразу рассмотрим конкретный пример. Пусть мы имеем структуру сети, приведенную на рисунке :



Часть данных «будем опускать» т.к. в данном «рецепте» они не существенны – например, имя внутреннего сетевого интерфейса на сервере или конкретный ip адрес внешнего интерфейса нам «не нужны для рассмотрения».

Подразумевается только что никакие настройки «не конфликтуют» и все корректно указано.

У сервера 2 интерфейса, один внешний (eth2) и внутренний – 10.0.0.1, маска 255.255.255.0. На сервере указаны в качестве DNS серверов 2 ip адреса – dns-ip1 и dns-ip2.

Клиенты подключены к внутренней сети и имеют адреса вида 10.0.0.xxx

(*предполагается, что на сервере доступа DNS-сервер не функционирует и мы используем сервера провайдера*)

4. Настройка клиентов

Это самое простое, потому просто «отметим это» чтобы «не возвращаться потом».

Настройка клиентов заключается в **прописывании у них в качестве шлюза** по умолчанию – внутреннего интерфейса сервера (10.0.0.1); и **указании DNS серверов** - тех же серверов что и у самого сервера доступа (dns-ip1 и dns-ip2).

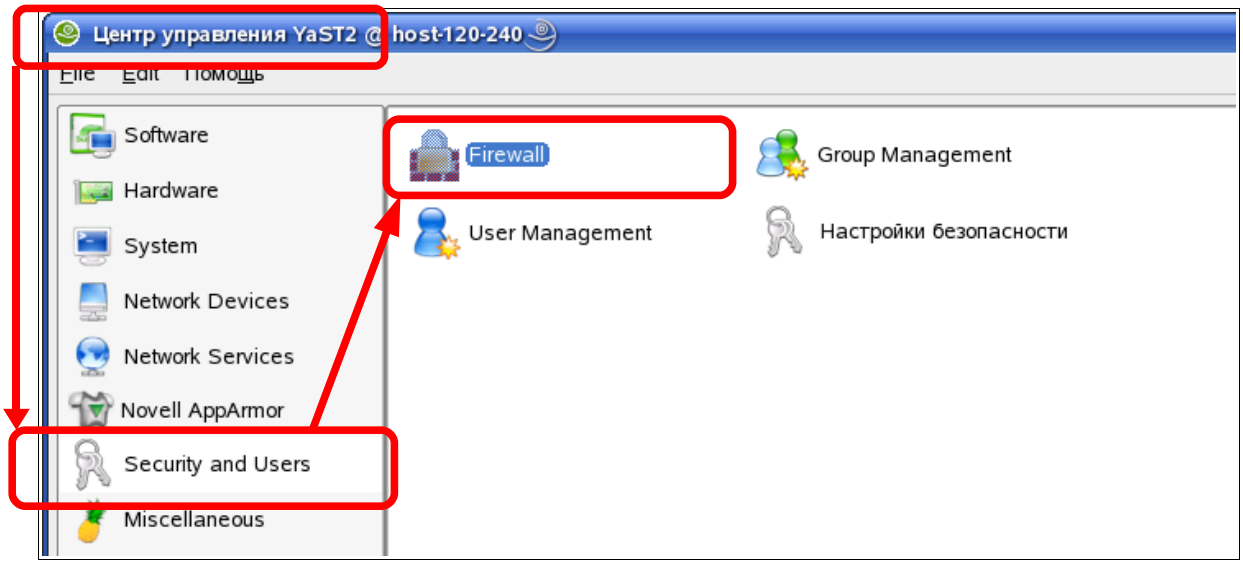
5. Настройка сервера.

Собственно состоит из 2-х шагов -

1) Вы должны **определить зоны принадлежности интерфейсов**. т.е. какой интерфейс принадлежит внешней зоне а какой к внутренней.

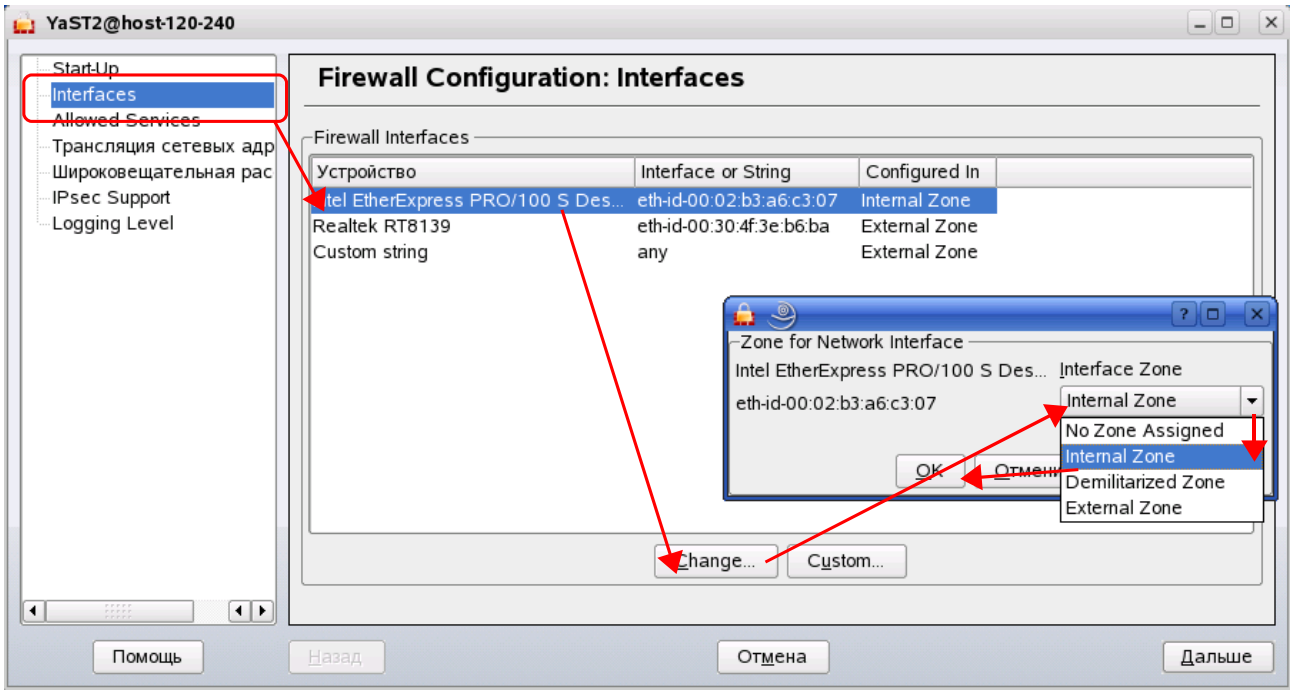
2) Вы должны **указать правила «маскарадинга», т.е.** указать какие конкретно порты надо «маскарадить» и куда .

Все это будем делать в настройках файрвола.
(откройте «YaSt», закладка «Security and users», апплет «Firewall»)



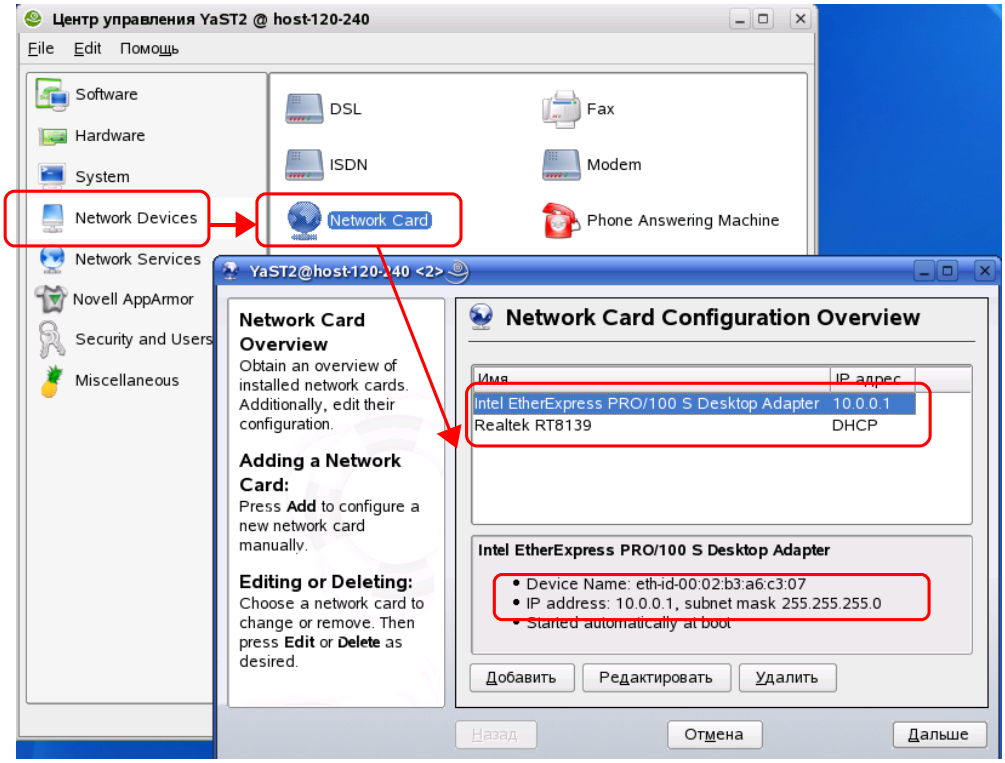
5.1 Определим зоны принадлежности интерфейсов

для того чтобы назначить интерфейсу зону нужно в настройках Firewall зайти на закладку «interfaces», выбрать интерфейс, нажать кнопку change, в появившемся меню выбрать зону, подтвердить свой выбор.



Интерфесу смотрящему во внешнюю сеть соответственно, назначаем «External zone»; интерфейсу в локальную сеть - «Internal zone». третьего не дано.

Как определить соответствие «устройства» здесь и «сетевого интерфейса»? Откройте параллельно настройку сетевых устройств и например сетевых карт и думаю все станет понятно.

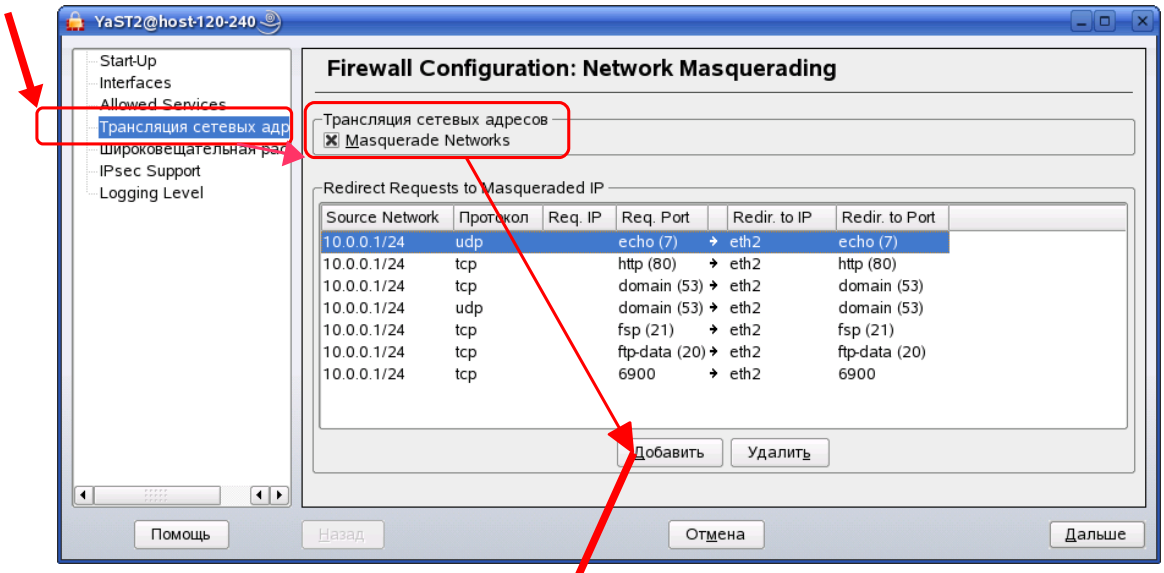


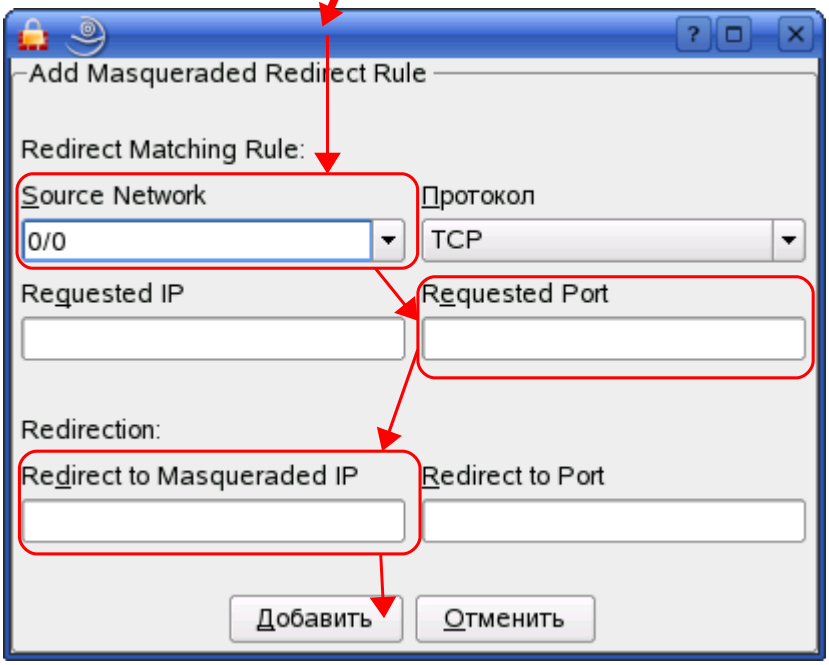
5.2 Создадим правила «Маскарадинга»

Для того чтобы определить правило маскарадинга для нашей задачи :

Надо открыть закладку трансляция сетевых адресов (в настройках SuSe Firewall), проверить чтобы была «загнута галочка» «Maskquerade Networks», Нажать кнопку «Добавить», и в появившемся меню ввести параметры правила.

Для нашей задачи – дать доступ в инет внутренней сети – достаточно ввсети 3 параметра – сеть источник, запрашиваемый сервис (порт или «номер протокола») и внешний интерфейс или ip-адрес (от имени которого будут посылаться полученные запросы).





т.е. для того чтобы бегали «пинги» вводится следующее :

SourceNetwork	: 10.0.0.2\24
Protocol	: UDP
Requested port	: 7
Redirect to Maquearaded IP	: eth2

КСТАТИ, на картинке в начале страницы вы видите состояние правил после набора минимального джентельменского набора. (имхо автора)

Общая идея маскарадинга в нашем случае такова, что мы сопоставляем источник обращения, протокол, порт обращения и адрес, от имени которого этот запрос будет послан в сеть.

Таким образом мы открываем доступ к внешней сети только по определенному списку протоколов.

напомним порты ниболее часто используемых сервисов :

tcp 80 – http
udp 7 – «echo» (ping)
udp 53, tcp 53 – DNS
tcp 20, tcp 21 – ftp (passive mode)

Вообще – смотрите содержимое файла /ets/services и выбирайте что вам нравится. от себя добавлю :

tcp 6900 – RAGNAROK online. the game. ;)
tcp 5190 1080 440 – через них может работать ICQ а вообще – «оно» прекрасно работает и через 80-й порт. имхо, достаточно.

==========

Вот собственно и все. Подтверждайте изменения (кнопки «Дальше», «Принять») и после этих нехитрых махинаций на внутренних машинах должен появиться доступ к интернет.

==========

Ссылки.

http://keir.ru/HOWTO-SuSE_Masquerading.php

Вариант аналогичного руководства, но с ориентировкой для SuSe 10,1

http://linuxforum.ru

Тут много чего сказали что привело к появлению второй версии этого документа.

==========

Автор.

Denjs
2006.11.09_0310
icq# 169223130
e-mail: d p l s o f t @ m a i l . r u