netshe_alg

Original file

Универсальное программное обеспечение для сетевых устройств NETSHe.

Руководство пользователя

Преодоление NAT пользовательскими приложениями в NETSHe

Станислав Корсаков, ООО «Нетше лаб»

Одним из естественных применений NETSHe является использование встроенного межсетевого экрана для организации NAT (трансляции множества внутренних приватных адресов в один или несколько публичных внешних).

Напомним, что для самым простым и часто используемым вариантом NAT в NETSHe является PAT или маскарадинг (когда все внутренние адреса отображаются автоматическим образом в единственный внешний адрес). Кроме того, доступны варианты управляемого отображения внутренних адресов в более чем один внешний адрес, а также вариант NAT 1:1 (когда каждый внутренний адрес и порт отображается в заданный внешний адрес и порт и наоборот).

В любом случае, NAT обеспечивает корректную работу пользовательских приложений, функционирующих по схеме «запрос на внешний адрес-ответ».

Однако, кроме подобных приложений, существует значительное количество приложений типа голосовых и видео мессенджеров, игр, клиентов FTP и т. п., которые после регистрации на сервере (запроса к серверу) требуют наличия набора портов (отличающихся от порта запроса), для которых будет корректно настроен NAT, в том числе для пропуска трафика снаружи (от внешних адресов).

Примером таких приложений является VoIP клиенты. Например, SIP-телефон, который после регистрации на сервере должен иметь возможность принять входящий вызов.

В отраслевой документации данный функционал можно встретить под аббревиатурой ALG (Application level gateway — шлюз уровня приложений).

В настоящем руководстве мы рассмотрим способы организации преодоления NAT для таких приложений.

Безусловно, написанное ниже имеет смысл только применительно к устройствам под управлением NETSHe и никоим образом не гарантирует преодоление любых других NAT между приложением и сервером / внешним приложением.

Автоматический способ

Очевидно, что наилучшим способом для пользователя является тот способ, в котором все делается без его участия / без настроек.

Такой способ имеется в NETSHe и присутствует в некоторых вариантах / сборках встроенного ПО.

Автоматический способ не требует никакой дополнительной настройки, поддерживает некоторые, наиболее распространенные протоколы: H323, SIP, PPTP, RTSP, FTP и т. п.

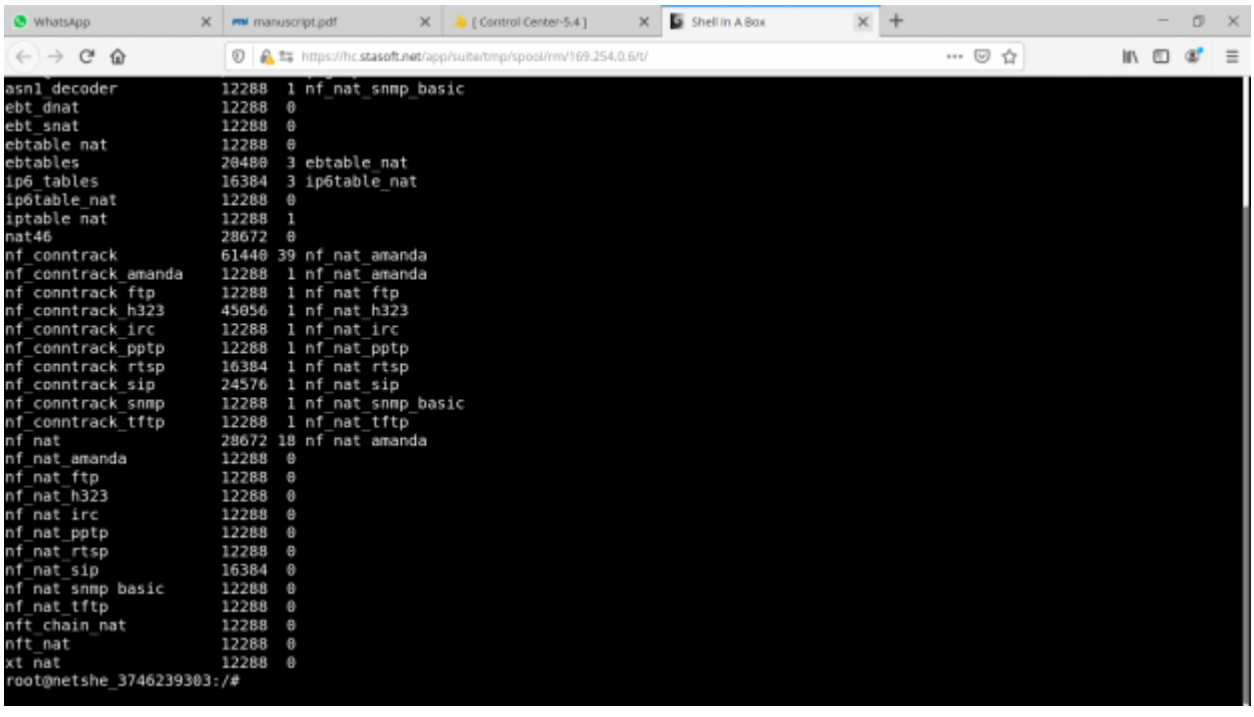
Обеспечивается вспомогательными модулями межсетевого экрана, которые анализируют проходящие пакеты на предмет соответствия протоколу, выбирают из них необходимую информацию об адресах и требуемых портах и конструируют записи для таблиц трансляции с соответствующими значениями TTL.

Как проверить что вспомогательный модуль для протокола есть в прошивке?

Для проверки доступности автоматической трансляции адресов следует подключиться к консоли устройства любым доступным способом:

- SSH;
- Telnet;
- Веб-консоль;
- Физическая консоль.

Дать команду *lsmod | grep nat*

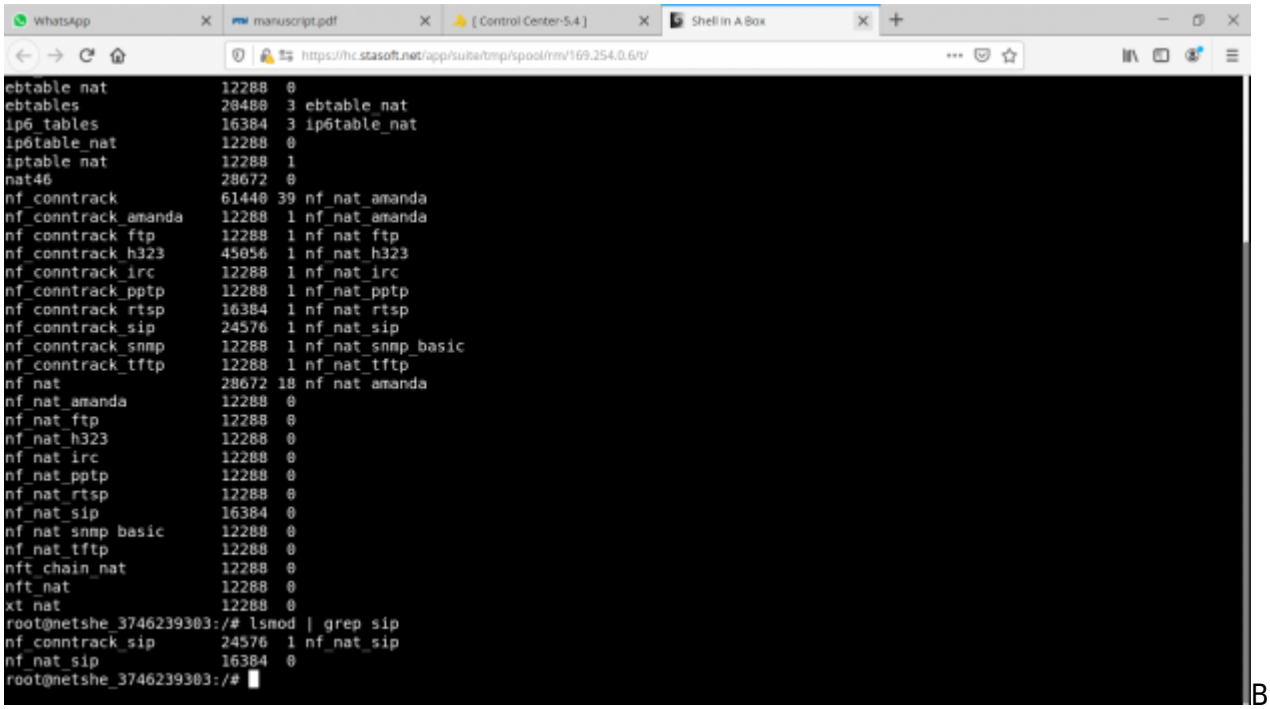


Вывод команды показан на рисунке выше.

Как можно видеть, в выводе присутствуют модули, содержащие слово „nat“ и названия

протоколов в имени. Из чего следует сделать вывод о доступности автоматической поддержки ALG в составе ПО.

Для того, что бы убедиться, что автоматическая поддержка ALG доступна для интересующего протокола (например, SIP), следует дать в консоли команду *lsmod | grep sip*



Вывод, свидетельствующий о наличии автоматической поддержки ALG для протокола SIP.

Как можно видеть на рисунке выше, загружены два модуля nf_conntrack_sip и nf_nat_sip, реализующие автоматический ALG для SIP.

Кроме отсутствия настроек, автоматический способ позволяет не заботиться об использовании фиксированных адресов и портов приложений / клиентов во внутренней сети. Записи для трансляции формируются исходя из текущих адресов и портов.

Обобщая, нужно заметить, что автоматическая поддержка ALG для протокола доступна при наличии двух модулей с именами nf_conntrack_ИМЯПРОТОКОЛА и nf_nat_ИМЯПРОТОКОЛА.

Необходимо отметить, что наличие автоматической поддержки ALG для протокола, не гарантирует корректную работу приложения.

Для некоторых приложений помощь в преодолении NAT может оказать использование UPnP прокси и (или) внешнего STUN сервера.

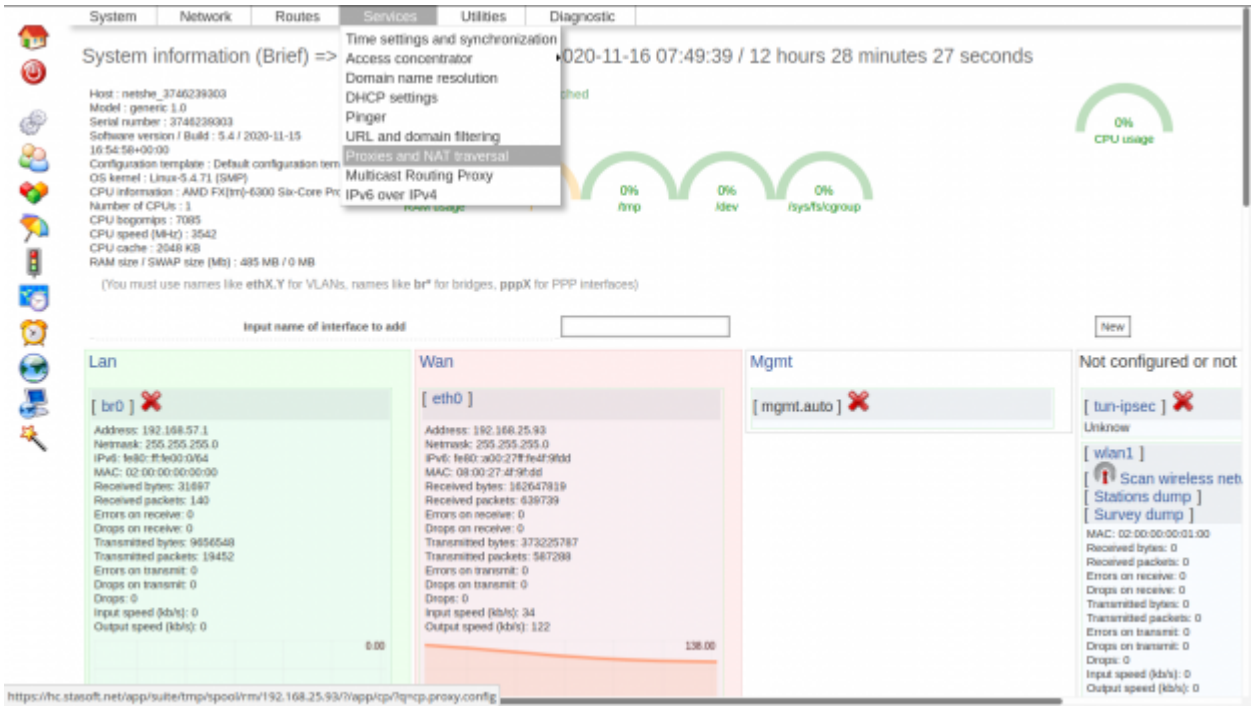
UPnP и STUN

Встроенное ПО на базе NETSHe может содержать средства преодоления NAT с помощью UPnP прокси и (или) внешнего STUN-сервера.

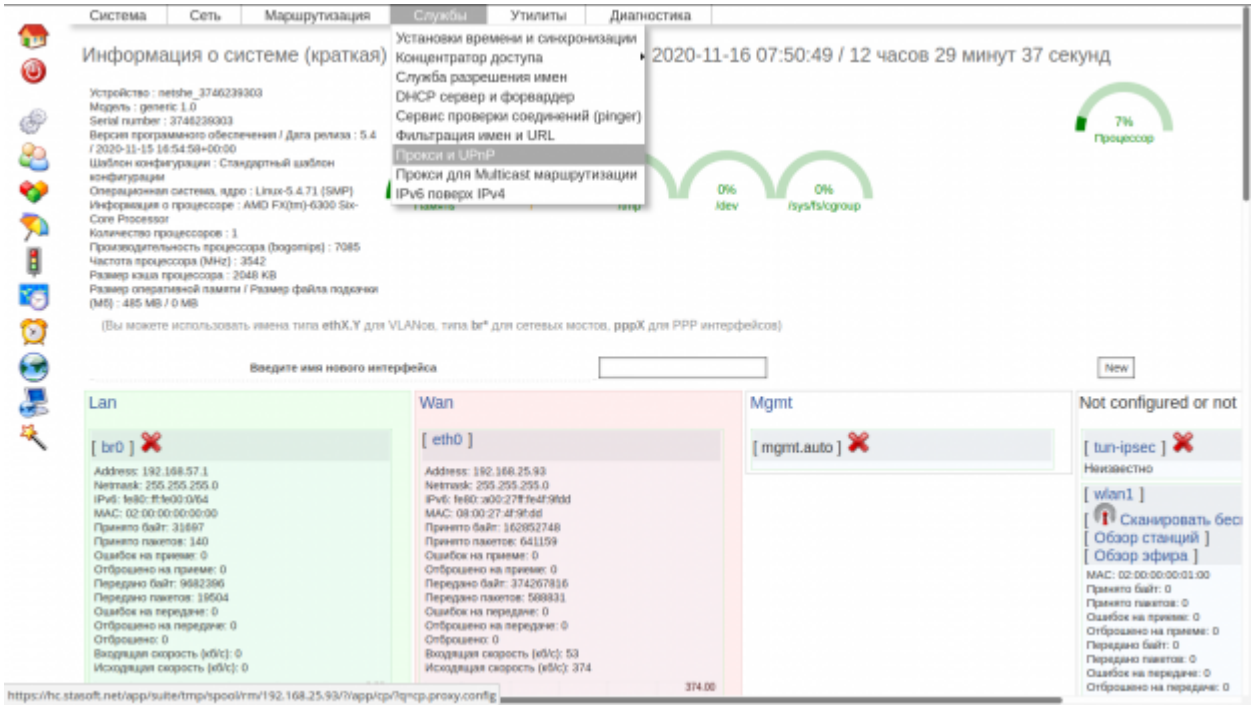
Использование UPnP требует сделать некоторые первоначальные настройки, однако, как и в автоматическом случае не требует фиксации внутренних адресов и портов приложений.

Соответствующие записи в таблице трансляции вносятся автоматически по запросу приложения.

Для настройки UPnP выберите меню «Services→Proxies and NAT traversal» в англоязычном интерфейсе

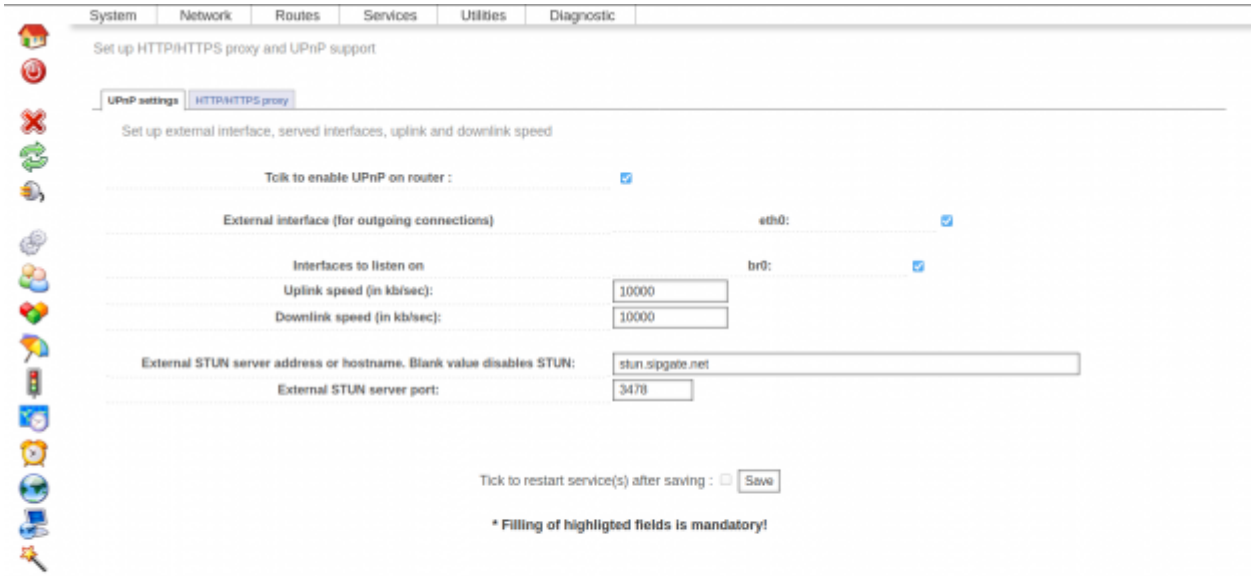


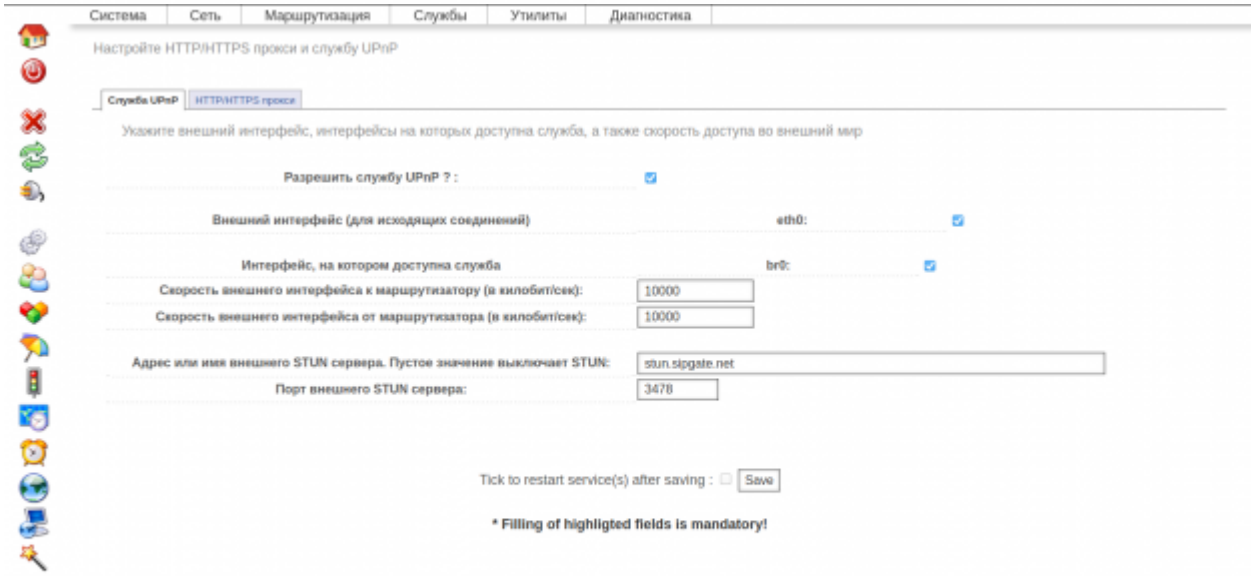
Или меню «Службы→Прокси и UPnP» в русскоязычном.



Настройка UPnP заключается в разрешении службы, указании внешнего интерфейса (Wan), внутреннего интерфейса (Lan), скорости подключения к внешнему маршрутизатору и указанию (необязательному) адреса или имени внешнего STUN сервера и его порта.

После ввода данных, службу следует перезапустить.





В качестве свободно доступных STUN серверов можно использовать следующие:

stun.l.google.com:19302
stun1.l.google.com:19302
stun2.l.google.com:19302
stun3.l.google.com:19302
stun4.l.google.com:19302
stun01.sipphone.com
stun.ekiga.net
stun.fwdnet.net
stun.ideasip.com
stun.iptel.org
stun.rixtelecom.se

stun.schlund.de
stunserver.org
stun.softjoys.com
stun.voiparound.com
stun.voipbuster.com
stun.voipstunt.com
stun.voxgratia.org

stun.xten.com

STUN-сервер полезно использовать для преодоления NAT голосовыми и видео-мессенджерами, средствами VoIP телефонии, конференц-связи.

Следует помнить, что STUN-сервер, скорее всего, окажется бесполезным при наличии примитивного NAT между маршрутизатором с NETSHe и внешним приложением, либо при наличии приватного IP-адреса на внешнем интерфейсе маршрутизатора с NETSHe.

Ручной способ с настройкой проброса портов

Третьим способом настройки преодоления NAT является настройка проброса портов на межсетевом экране NETSHe.

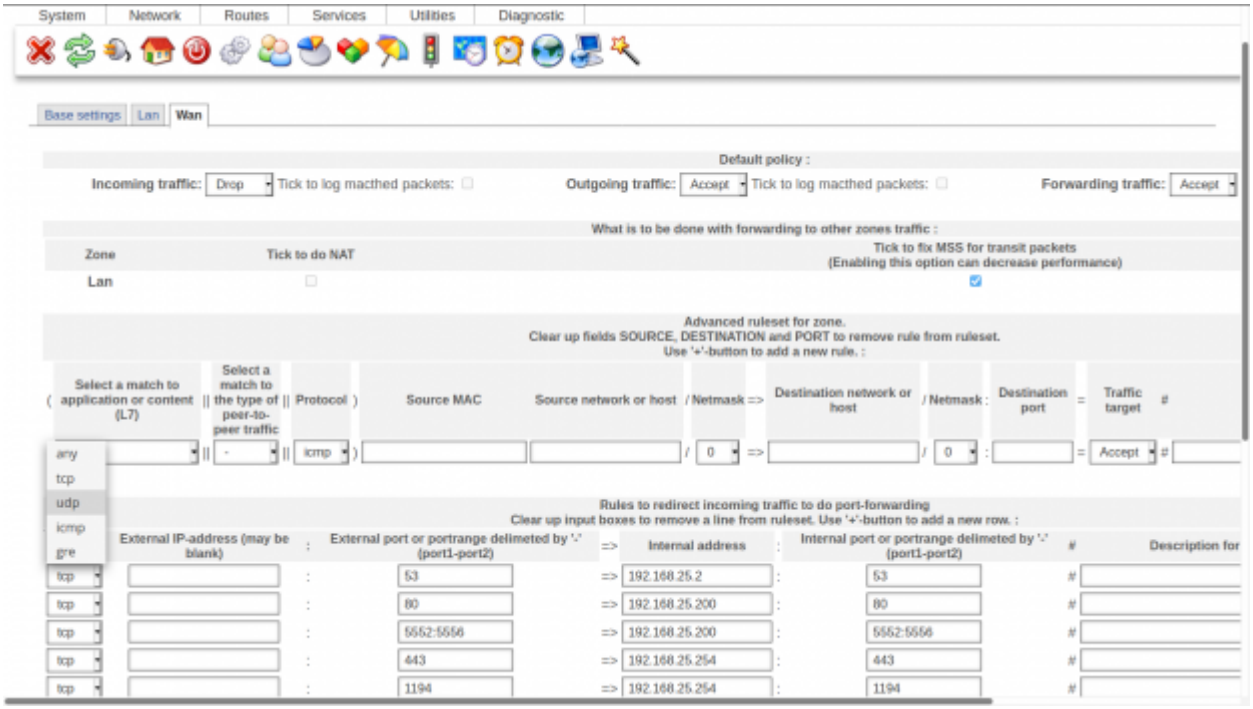
Является самым трудоемким в настройке способом (требуется настройка как МСЭ, так и приложения), требует фиксации адреса и портов приложения (например, VoIP телефон должен иметь конкретный адрес и использовать оговоренный набор портов).

Кроме того, данный способ ограничивает число доступных приложений за NAT (например, не более одного SIP-телефона при PAT).

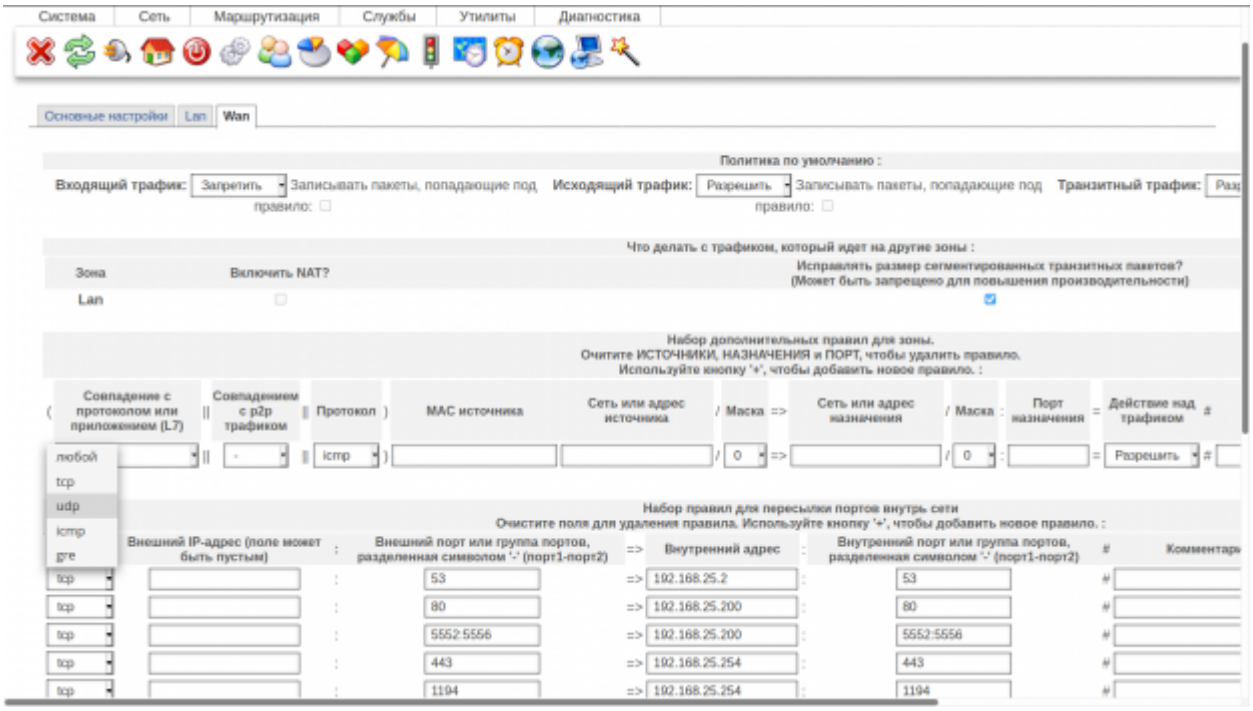
Достоинством метода является гарантированное преодоление NAT даже при некорректной работе автоматических модулей, отсутствии поддержки STUN и UPnP в приложении.

Для настройки проброса портов, пожалуйста, используйте руководство по межсетевому экрану NETSHe.

Для настройки следует выбрать меню «Network→Firewall», закладку «Wan» в английской версии интерфейса



Или меню «Сеть→Межсетевой экран», закладку «Wan»



Следует использовать секцию «Набор правил для пересылки портов внутрь сети» / «Port forwarding», где добавить правила для протокола, внешнего порта (или диапазона портов), внутреннего адреса (куда пересылать порт(ы)) и внутреннего порта (диапазона портов).