

netshe_alg

[Original file](#)

Универсальное программное обеспечение для сетевых устройств NETSHe.

Руководство пользователя

Преодоление NAT пользовательскими приложениями в NETSHe

Станислав Корсаков, ООО «Нетше лаб»

(с) 2009-2020 Ярославль

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

Напомним, что для самым простым и часто используемым вариантом NAT в NETSHe является PAT или маскардинг (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.

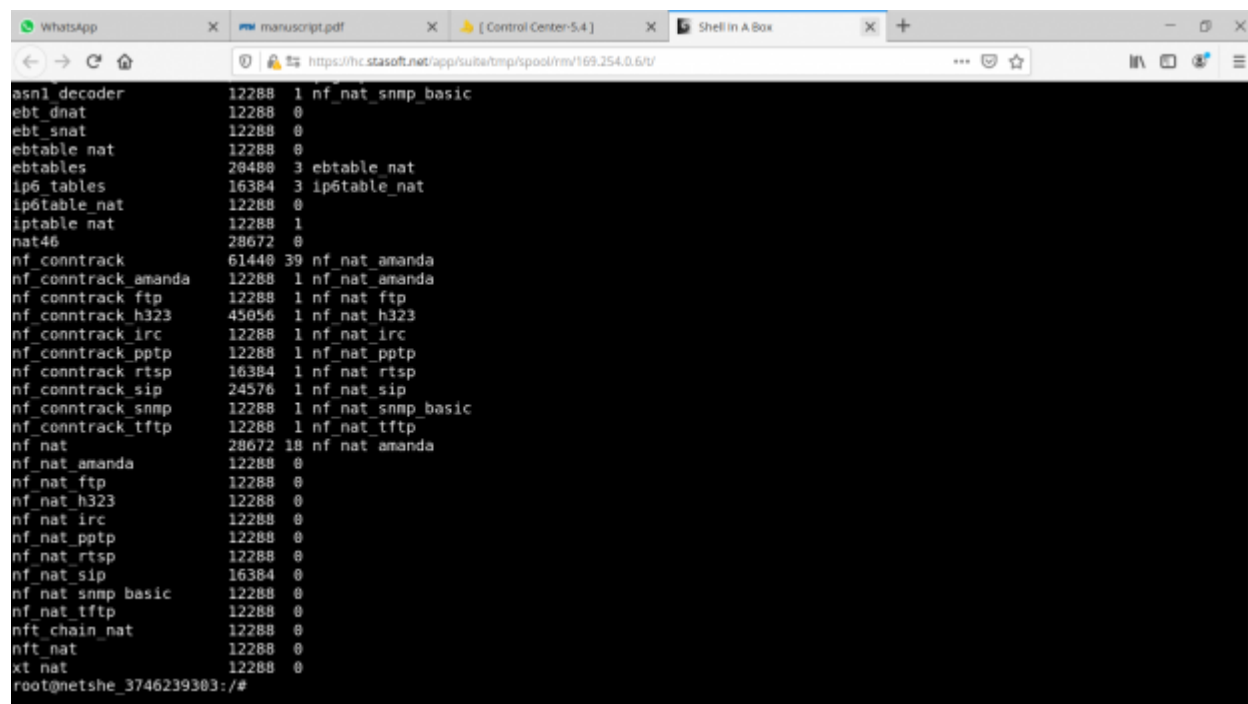
Обеспечивается вспомогательными модулями межсетевого экрана, которые анализируют проходящие пакеты на предмет соответствия протоколу, выбирают из них необходимую информацию об адресах и требуемых портах и конструируют записи для таблиц трансляции с соответствующими значениями TTL.

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`



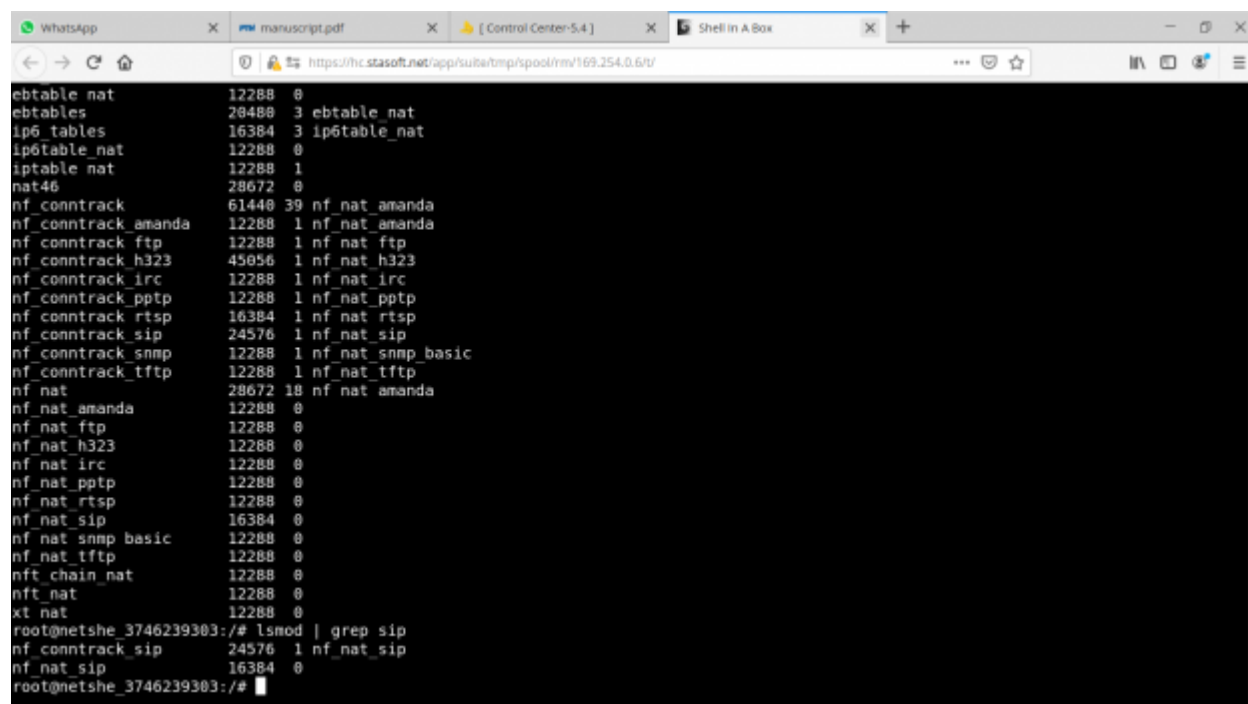
```
asn1_decoder 12288 1 nf_nat_snmp_basic
ebt_dnat 12288 0
ebt_snat 12288 0
ebtable_nat 12288 0
ebtables 28480 3 ebtable_nat
ip6_tables 16384 3 ip6table_nat
ip6table_nat 12288 0
iptable_nat 12288 1
nat46 28672 0
nf_conntrack 61440 39 nf_nat_amanda
nf_conntrack_amanda 12288 1 nf_nat_amanda
nf_conntrack_ftp 12288 1 nf_nat_ftp
nf_conntrack_h323 45056 1 nf_nat_h323
nf_conntrack_irc 12288 1 nf_nat_irc
nf_conntrack_pptp 12288 1 nf_nat_pptp
nf_conntrack_rtsp 16384 1 nf_nat_rtsp
nf_conntrack_sip 24576 1 nf_nat_sip
nf_conntrack_snmp 12288 1 nf_nat_snmp_basic
nf_conntrack_tftp 12288 1 nf_nat_tftp
nf_nat 28672 18 nf_nat_amanda
nf_nat_amanda 12288 0
nf_nat_ftp 12288 0
nf_nat_h323 12288 0
nf_nat_irc 12288 0
nf_nat_pptp 12288 0
nf_nat_rtsp 12288 0
nf_nat_sip 16384 0
nf_nat_snmp_basic 12288 0
nf_nat_tftp 12288 0
nft_chain_nat 12288 0
nft_nat 12288 0
xt_nat 12288 0
root@netshe_3746239303:/#
```

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`



```

ehtable nat          12288  0
ehtable             28480  3 ehtable_nat
ip6_tables          16384  3 ip6table_nat
ip6table_nat        12288  0
iptable nat         12288  1
nat46               28672  0
nf_conntrack        61440 39 nf_nat_amanda
nf_conntrack_amanda 12288  1 nf_nat_amanda
nf_conntrack_ftp    12288  1 nf_nat_ftp
nf_conntrack_h323   45056  1 nf_nat_h323
nf_conntrack_irc    12288  1 nf_nat_irc
nf_conntrack_pptp   12288  1 nf_nat_pptp
nf_conntrack_rtsp   16384  1 nf_nat_rtsp
nf_conntrack_sip    24576  1 nf_nat_sip
nf_conntrack_snmp   12288  1 nf_nat_snmp_basic
nf_conntrack_tftp   12288  1 nf_nat_tftp
nf_nat              28672 18 nf_nat_amanda
nf_nat_amanda       12288  0
nf_nat_ftp           12288  0
nf_nat_h323          12288  0
nf_nat_irc           12288  0
nf_nat_pptp          12288  0
nf_nat_rtsp          12288  0
nf_nat_sip           16384  0
nf_nat_snmp_basic    12288  0
nf_nat_tftp          12288  0
nft_chain_nat        12288  0
nft_nat              12288  0
xt_nat               12288  0
root@netshe_3746239303:~# lsmod | grep sip
nf_conntrack_sip    24576  1 nf_nat_sip
nf_nat_sip          16384  0
root@netshe_3746239303:~#

```

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.

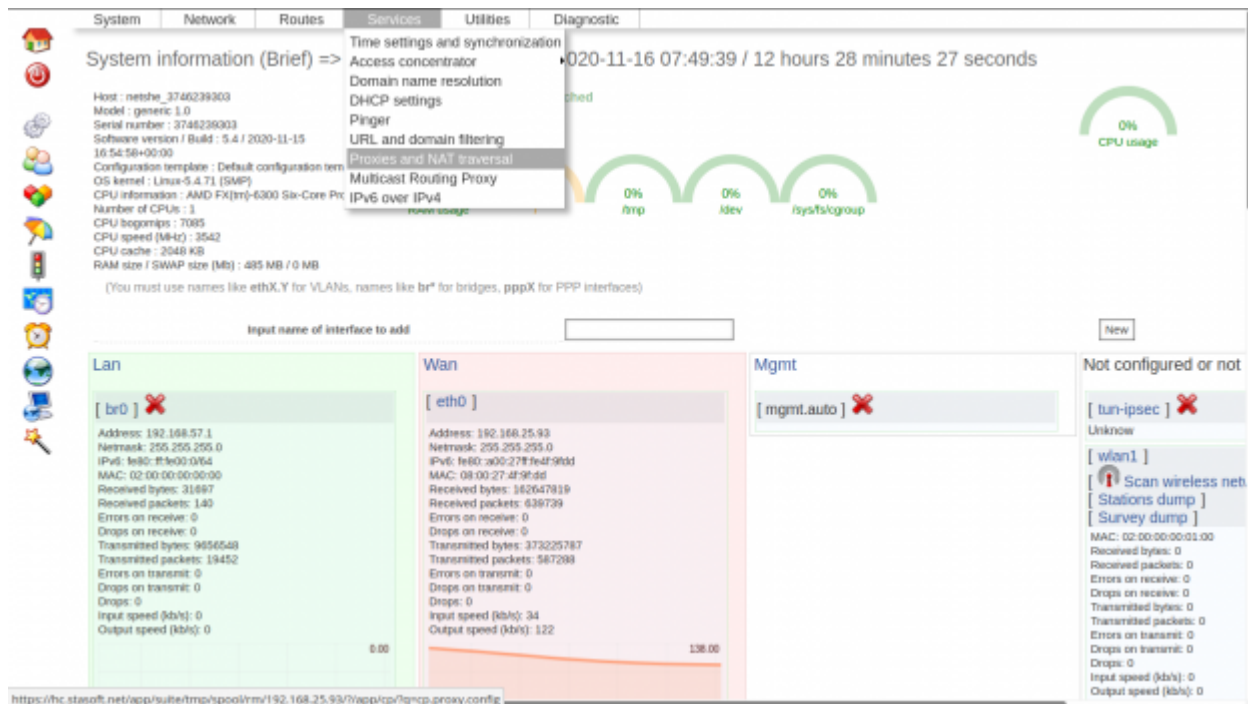
UPnP и STUN

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

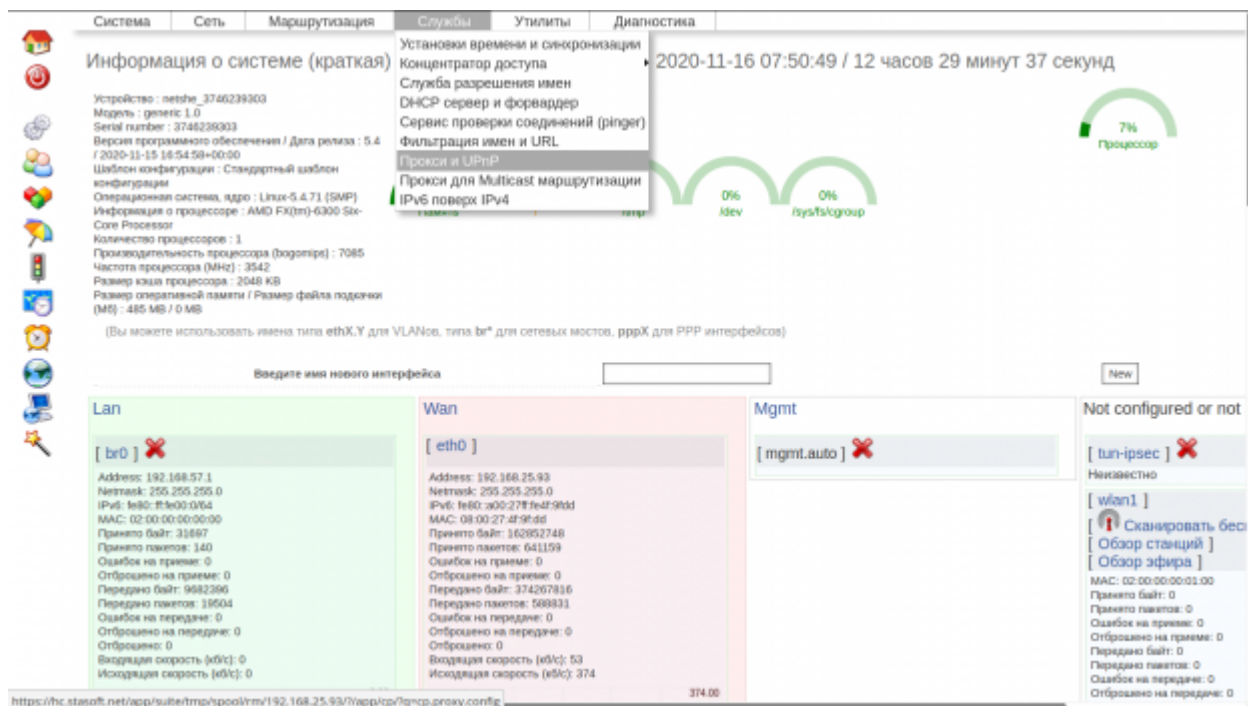
Использование UPnP требует сделать некоторые первоначальные настройки, однако, как и в автоматическом случае не требует фиксации внутренних адресов и портов приложений.

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 (необязательно) адреса или имени внешнего STUN сервера и его порта.

После ввода данных, службу следует перезапустить.

System Network Routes Services Utilities Diagnostic

Set up HTTP/HTTPS proxy and UPnP support

UPnP settings HTTP/HTTPS proxy

Set up external interface, served interfaces, uplink and downlink speed

Tick to enable UPnP on router : ☒

External interface (for outgoing connections) eth0: ☒

Interfaces to listen on br0: ☒

Uplink speed (in kb/sec): 10000

Downlink speed (in kb/sec): 10000

External STUN server address or hostname. Blank value disables STUN: stun.sipgate.net

External STUN server port: 3478

Tick to restart service(s) after saving : ☐ Save

* Filling of highlighted fields is mandatory!

Система Сеть Маршрутизация Услуги Утилиты Диагностика

Настройте HTTP/HTTPS прокси и службу UPnP

Служба UPnP HTTP/HTTPS прокси

Укажите внешний интерфейс, интерфейсы на которых доступна служба, а также скорость доступа во внешний мир

Разрешить службу UPnP ? : ☒

Внешний интерфейс (для исходящих соединений) eth0: ☒

Интерфейс, на котором доступна служба br0: ☒

Скорость внешнего интерфейса к маршрутизатору (в килобит/сек): 10000

Скорость внешнего интерфейса от маршрутизатора (в килобит/сек): 10000

Адрес или имя внешнего STUN сервера. Пустое значение выключает STUN: stun.sipgate.net

Порт внешнего STUN сервера: 3478

Tick to restart service(s) after saving : ☐ Save

* Filling of highlighted fields is mandatory!

B

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

System Network Routes Services Utilities Diagnostic

Base settings Lan Wan

Default policy :

Incoming traffic: Drop Tick to log matched packets: ☐ Outgoing traffic: Accept Tick to log matched packets: ☐ Forwarding traffic: Accept

What is to be done with forwarding to other zones :

Zone	Tick to do NAT	Tick to fix MSS for transit packets (Enabling this option can decrease performance)
Lan	☐	☒

Advanced ruleset for zone.
Clear up fields SOURCE, DESTINATION and PORT to remove rule from ruleset.
Use '+'-button to add a new rule. :

Select a match to application or content (L7)	Select a match to the type of peer-to-peer traffic	Protocol	Source MAC	Source network or host / Netmask	Destination network or host / Netmask	Destination port	Traffic target	#
any	-	icmp		/ 0			Accept	

Rules to redirect incoming traffic to do port-forwarding
Clear up input boxes to remove a line from ruleset. Use '+'-button to add a new row. :

External IP-address (may be blank)	External port or portrange delimited by '-' (port1-port2)	Internal address	Internal port or portrange delimited by '-' (port1-port2)	#	Description for
tcp	53	192.168.25.2	53	#	
tcp	80	192.168.25.200	80	#	
tcp	5552-5556	192.168.25.200	5552-5556	#	
tcp	443	192.168.25.254	443	#	
tcp	1194	192.168.25.254	1194	#	

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

Система Сеть Маршрутизация Службы Утилиты Диагностика

Основные настройки Lan Wan

Политика по умолчанию :

Входящий трафик: Запретить Записывать пакеты, попадающие под правило: ☐ Исходящий трафик: Разрешить Записывать пакеты, попадающие под правило: ☐ Транзитный трафик: Разрешить

Что делать с трафиком, который идет на другие зоны :

Зона	Включить NAT?	Исправить размер сегментированных транзитных пакетов? (Может быть запрещено для повышения производительности)
Lan	☐	☒

Набор дополнительных правил для зоны.
Очистите ИСТОЧНИКИ, НАЗНАЧЕНИЯ и ПОРТ, чтобы удалить правило.
Используйте кнопку '+', чтобы добавить новое правило. :

Совпадение с протоколом или приложением (L7)	Совпадением с p2p трафиком	Протокол	MAC источника	Сеть или адрес источника / Маска	Сеть или адрес назначения / Маска	Порт назначения	Действие над трафиком	#
любой	-	icmp		/ 0			Разрешить	

Набор правил для пересылки портов внутри сети
Очистите поля для удаления правила. Используйте кнопку '+', чтобы добавить новое правило. :

Внешний IP-адрес (поле может быть пустым)	Внешний порт или группа портов, разделенная символом '-' (port1-port2)	Внутренний адрес	Внутренний порт или группа портов, разделенная символом '-' (port1-port2)	#	Комментарий
tcp	53	192.168.25.2	53	#	
tcp	80	192.168.25.200	80	#	
tcp	5552-5556	192.168.25.200	5552-5556	#	
tcp	443	192.168.25.254	443	#	
tcp	1194	192.168.25.254	1194	#	

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

From:
<http://docs.netshe-lab.ru/> - Документация по NETSHe

Permanent link:
http://docs.netshe-lab.ru/doku.php?id=%D0%BF%D1%80%D0%B5%D0%BE%D0%B4%D0%BE%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_nat_alg_%D0%B2_netshe

Last update: 2020/11/16 07:57

