Команда nat

Содержание

Описание

NAT - модуль преобразования сетевых адресов (Network Address Translation, RFC1631). Позволяет в какой-то мере решить проблему исчерпания пространства адресов в IPv4 за счёт изменения IP-адресов локальной сети на общедоступный адрес (public address), с указанием порта таким образом, чтобы можно было безошибочно идентифицировать адресата данных, при их возвращении обратно.

ВНИМАНИЕ

В качестве локальных адресов может использоваться часть адресного пространства IPv4, зарезервированная для применения в так называемых частных IP-сетях (private internets). Протоколы маршрутизации глобальной сети Интернет не передают информацию об этих адресах, что позволяет использовать одни и те же адреса в разных местах глобальной сети. Частные сети широко используются провайдерами или компаниями для построения внутренней транспортной среды, а также для подключения небольших групп абонентов.

```
10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
```

Синтаксис:

Title

```
local_acl        (-acl) - ACL local networks list and public address
                          argument: $NAME [public_addr|dhcp IFNAME]
                                [-exclude $DSTACL] [enable|disable|delete]
maxlinks         (-ml ) - maximal links number
                          argument: NUM
ignore_incoming  (-i  ) - ignore unknown incoming connections
                          argument: [yes|no]
same_ports       (-sp ) - try to keep original port numbers for connections
                          argument: [yes|no]
verbose          (-v  ) - verbose mode, dump packet information
                          argument: [yes|no]
stat             (-s  ) - NAT statistic
redirect_port    (-rpo) - redirect a port (or ports) for incoming traffic
                          argument: tcp|udp|ras|cs local_addr:local_port_range[,...]
                          [public_addr:]public_port_range
                          [remote_addr[:remote_port_range]]
redirect_proto   (-rpr) - redirect packets of a given proto
                          argument: proto local_addr [public_addr [remote_addr]]
redirect_address (-ra ) - define mapping between local and public addresses
                          argument: local_addr[,...] public_addr
proxy_rule       (-pr ) - add transparent proxying / destination NAT
                          argument:
                          [type encode_ip_hdr|encode_tcp_stream]
                          [port xxxx]
                          [server [a.b.c.d]:yyyy]
                          [proto tcp|udp] [src <addr>[/mask]] [dst <addr>[/mask]]
default_h323     (-dh ) - use default H.323 ports for outgoing connections
                          argument: [yes|no]
h323_destination (-hd ) - describe H.323 outgoing connection
                          argument: ras|cs remote_addr[:remote_port]
                          [local_addr[:local_port]]
proxy_only       (-po ) - transparent proxy only, no aliasing
                          argument: [yes|no]
skinny_port      (-skp) - set the TCP port for the Skinny Station protocol
                          argument: port
del              (-del) - delete nat rule
                          argument: rule_number
enable           (ena ) - enable nat translation
disable          (disa) - disable nat translation
```

Параметры

Параметр	Описание

local_acl $NAME [public_addr|dhcp IFNAME] [-exclude $DSTACL] [enable|disable|delete]	Общедоступный (public) IP-адрес, который будет использоваться для трансляции адресов, назначается физическому интерфейсу маршрутизатора командой *"ifconfig"*. Маршрутизаторы "Инфинет" имеют как минимум два физических интерфейса: ethernet (eth) и radio (rf). Обычно через радиоинтерфейс блок доступа подключен к опорной сети провайдера, которая, скорее всего, также построена на частных IP-адресах. Ethernet используется для подключения вашей локальной сети и, следовательно будет иметь один из частных адресов вашей локальной сети. **ВНИМАНИЕ** Иногда можно не назначать общедоступный адрес на интерфейсы маршрутизатора. Обеспечить доступность данного адреса со стороны глобальной сети можно с помощью статической маршрутизации. Провайдер может описать маршрут на этот адрес так, чтобы пакеты, направляющиеся на него, попадали на ваш блок доступа. Модуль NAT выполнит преобразование раньше чем система идентифицирует, ей ли адресован пакет. По отношению к другим компонентам системы модуль NAT встроен таким образом, что всегда используются действительные адреса источника и приёмника. То есть, например, при составлении правил "*ipfw"* следует оперировать локальными адресами внутренней сети. Они же будут показаны при сборе статистики модулем "*ipstat"*. Имя списка (ACL) локальных сетей, которые требуют трансляции адресов, задаётся при помощи команды "acl". После чего с помощью параметра"*local_acl*" для этого списка может быть назначен один из общедоступных IP-адресов. Все пакеты с адресами источников, попадающими в список "local_acl", считаются исходящими и подлежат преобразованию. Исключение составляют пакеты, проходящие из "local_acl" в сеть из того же списка "local_acl", а также из сети списка "local_acl" на собственные адреса маршрутизатора. Эти и все остальные пакеты считаются входящими и, если они не являются обратными к уже преобразованным соединениям, пропускаются насквозь без изменения. • *"$NAME"* – имя списка локальных сетей, которые требуют трансляции адресов. • "*public_addr*" – общедоступный IP-адрес, который будет использоваться для трансляции адресов. • "*dhcp IFNAME*" – адрес, полученный по протоколу DHCP. Требуется так же указать интерфейс, через который DHCP выдал адрес. • *"-exclude $DSTACL"* – список адресатов/сетей, не требующих трансляции адресов. • "*enable*"/"*disable*"/"*delete*" – позволяют сделать данную запись рабочей/нерабочей/удалить её.
maxlinks NUM	Задаёт максимальное количество поддерживаемых соединений, по умолчанию 1000. Система следит за состоянием соединений и динамически освобождает ненужные в зависимости от их типа, времени действия и активности. Однако, при работе различных сканеров сети может возникнуть ситуация, когда количество соединений будет расти до бесконечности или пока не кончится оперативная память. С помощью этой команды можно предотвратить бесконтрольное и неограниченное распределение оперативной памяти маршрутизатора. В случае, когда количество одновременных соединений превысит установленный предел, система выведет предупреждение в системный журнал и запретит создание новых соединений, пока ситуация не нормализуется. Когда количество соединений вернётся в норму, в системный журнал будет сделана соответствующая запись, и работа возобновится.
"enable"	Разрешает модулю NAT выполнять трансляцию адресов в соответствии с установленными правилами.
"disable"	Прекращает трансляцию адресов, но сохраняет все ранее введённые параметры NAT.
same_ports [yes|no]	Если данная опция включена, модуль NAT стремится оставлять номера портов в преобразуемых пакетах без изменений. Если это становится невозможным, то будут использоваться произвольные номера из числа доступных. Опция включена по умолчанию. • *"yes"/"no"* – включение/отключение опции.
verbose [yes|no]	Включает режим диагностики и выводит содержимое всех обрабатываемых пакетов и их изменения в системный журнал.
proxy_only [yes|no]	Включает режим, в котором модуль NAT выполняет только функции перенаправления пакетов, заданные командами "*proxy_rule"*. Обычная трансляция адресов не выполняется.
stat	Выводит статистику текущей работы со всеми активными каналами преобразования.
ignore_incoming [yes|no]	Включает/отключает игнорирование неизвестных входящих соединений.
skinny_port port	Устанавливает порт TCP для протокола Skinny. Skinny используется IP-телефонами Cisco для работы с Cisco Call Managers. Если данные не заданы, команда "*Skinny aliasing*" не будет выполнена. Стандартный порт, используемый Skinny, - 2000.

default_h323 [yes|no]	Включает изменение адресов в соответствии со стеком H.323 для исходящих соединений. Обрабатываются все UDP-пакеты, исходящие на порт 1719, и TCP-потоки, исходящие на порт 1720. По умолчанию отключена. **ПРЕДОСТЕРЕЖЕНИЕ** Не стоит без необходимости включать эту опцию, так как с этой опцией NAT будет обрабатывать все UDP-пакеты, исходящие на порт 1719, и TCP-потоки, исходящие на порт 1720, что замедлит работу NAT при использовании этих портов и протоколов не для телефонии H.323.
h323_destination ras|cs remote_addr[:remote_port] [local_addr[:local_port]]	Детально описывает использование элементов H.323 во внешней сети, осуществляя обработку потоков H.323. Чтобы лучше разобраться в настройке данного параметра, изучите примеры в подразделе "NAT и H.323 телефония". • "*ras|cs*" - слой стека H.323, для которого будет выполняться обработка. • "*remote_addr*" - адрес внешней сети, исходящие соединения на который будут обрабатываться. • "*remote_port*" - порт, исходящие соединения на который будут обрабатываться. Если порт не указан, то используется порт 1719 для RAS и 1720 для CS. • "*local_addr*" - адрес внутренней сети, исходящие соединения с которого будут обрабатываться. Если адрес не указан, то обрабатываются соединения, исходящие с любого адреса. • "*local_port*" - порт, исходящие соединения с которого будут обрабатываться. Если порт не указан, то обрабатываются соединения, исходящие с любого порта.
del rule_number	Удаляет правило с номером "*rule_number*" при просмотре конфигурации *"config show".*
Перенаправление пакетов	
redirect_port proto local_addr:local_port_range [public_addr:]public_port_range [remote_addr[:remote_port_range]]	Обеспечивает перенаправление некоторых портов машины с NAT на клиента локальной сети, с целью нивелировать минусы использования NAT при запуске служб сети интернет на клиентских машинах в локальной сети. Допускается многократное выполнение команд с различными аргументами, каждая команда добавляет правило в общий список. При просмотре конфигурации "*config show*" команды перенаправления пакетов будут пронумерованы. Это дает возможность удалять ненужные правила из списка командами "*nat del XX*", где "*XX*" порядковый номер правила по конфигурации. • "*proto*" – аргумент, определяющий протокол, может принимать значения *"tcp", "udp", "ras"* или *"cs"*. В случае *"ras"* или *"cs"* осуществляется изменение адресов в соответствии со стеком H.323. • *"local_addr:local_port_range"* – задаёт IP-адрес и порт машины в локальной сети. Во второй форме команды заменяется на "*local_addr_1:local_port_range[, local_addr_2:local_port_range, ...]*", что позволяет выполнить циклическую пересылку входящих пакетов по нескольких адресам (LSNAT) для распределения нагрузки между ними. • "*[public_addr:]public_port_range*" – задаёт общедоступный IP-адрес и порт. В случае одновременного использования нескольких пар "общедоступный адрес - частная сеть" рекомендуется указывать конкретный общедоступный адрес. • "*[remote_addr[:remote_port_range]]*" – задаётся для более точного определения входящих соединений (будут обрабатываться только пакеты, приходящие с указанного адреса и порта). Если "*remote_port_range*" не указан, то подразумеваются любые порты. Если "*remote_port_range*" указан, то его размер должен совпадать с диапазоном "*public_port_range*". **ВНИМАНИЕ** Диапазоны портов "*public_port_range*" и "*local_port_range*" обязаны быть одинакового размера.
redirect_address local_addr[,...] public_addr	Перенаправляет весь входящий трафик, поступающий на общедоступный адрес (public), на адрес машины в локальной сети. Если указано несколько адресов, то перенаправление будет выполняться поочерёдно на каждый адрес по кругу. Перенаправление адреса полезно, если имеется несколько адресов IP, и они должны быть на одной машине. В этой ситуации NAT может назначить каждому клиенту сети свой собственный внешний IP-адрес. Затем NAT преобразует исходящие от клиентов локальной сети пакеты, заменяя IP-адреса на соответствующие внешние, и перенаправляет весь трафик, входящий на некоторый IP-адрес, обратно конкретному клиенту локальной сети. Это также называют статическим NAT. Внешние IP-адреса машины с NAT должны быть активизированы и быть алиасами для внешнего интерфейса, либо должны быть описаны иным способом.
redirect_proto proto local_addr [public_addr [remote_addr]]	Перенаправляет все входящие пакеты с типом протокола "proto" на машину с адресом в локальной сети. Если общедоступный IP-адрес не указан, используется значение параметра "*alias_address*" для соответствующей локальной сети. Если указан параметр "*remote_addr*", то обрабатываются только пакеты с этого адреса.

proxy_rule [type encode_ip_hdr|encode_tcp_stream] [port xxxx] [server [a.b.c.d]:yyyy] [proxy tcp|udp] [src <addr>[/mask]] [dst <addr>[/mask]]	Перенаправляет исходящие пакеты. TCP-пакеты, исходящие из локальной сети на любой адрес с указанным портом, перенаправляются на заданный сервер и порт. Командная строка состоит из одной или более пар слов, разделённых пробелами. Первое слово является ключевым параметром, второе его значением.
	• *"type"* –передает информацию о первоначальном адресе и порте доступа на новый сервер. Если это необходимо для организации прозрачного шлюза, то это может быть сделано двумя путями.
	  • "*encode_ip_hdr*", – при указании данной опции оригинальный адрес и порт передаются в расширенных полях заголовка IP (IP option).
	  • "*encode_tcp_stream*", – при указании данной опции оригинальный порт и адрес передаются в пакете перед началом данных в формате "*DEST IP port*".
	• *"port xxxx"* – позволяет ограничить обработку пакетов, отправленными на указанный порт.
	• *"[server [a.b.c.d]:yyyy]"* – обязательный параметр. Задаёт адрес сервера и порт, на который будут перенаправляться пакеты. Если порт не указан, то будет использоваться оригинальный порт назначения.
	• *"[proxy tcp|udp]"* – настраивает обработку пакетов только с заданным протоколом.
	• *"[src <addr>[/mask]]"* и *"[dst <addr>[/mask]]"* – задает адрес (подсеть) источника или назначения, для которых следует выполнять перенаправление пакетов.

Примеры

Назаначим общедоступный адрес "*123.1.1.1/32*" командой *"ifconfig"* на интерфейс *"rf5.0"*. Применим команду *"rip start"*, чтобы работала динамическая маршрутизация для общедоступный адреса.

```
ifconfig rf5.0 123.1.1.1/32 up
rip start
```

Создадим список с одной единственной сетью *"192.168.1.0/24"* (наша частная сеть) и назначим сетевой адрес *"123.1.1.1"* в качестве общедоступного адреса этой сети.

```
acl add $TEST net 192.168.1.0/24
nat local_acl $TEST 123.1.1.1
```

Либо в качестве общедоступного адреса используем адрес, полученный по протоколу DHCP. *"eth0"* – интерфейс, через который DHCP выдал адрес.

```
nat local_acl $TEST dhcp eth0
```

Разрешим модулю NAT выполнять трансляцию адресов в соответствии с установленными правилами.

```
nat enable
```

Выполним настройку, при которой все входящие соединения TCP на порт 7777 данного маршрутизатора будут перенаправляться на машину с адресом "*192.168.1.5*" и портом 23 (telnet).

```
nat redirect_port tcp 192.168.1.5:23  7777
```

Требуется задать диапазон портов так, чтобы все входящие пакеты TCP с портами назначения в диапазоне 3300-3399 и адресом назначения "*123.1.1.2*" перенаправлялись на машину "*192.168.1.4*". Преобразование портов выполняется 1:1, то есть 3300->2300, 3301->2301 и т.д.

```
nat redirect_port tcp 192.168.1.4:2300-2399 123.1.1.2:3300-3399
```

Пусть, к примеру, сервер IRC запущен на клиенте A, а веб-сервер работает на клиенте B. Чтобы это работало, соединения, принимаемые на портах 6667 (irc) и 80 (веб), должны перенаправляться на соответствующие машины.

```
nat redirect_port tcp 192.168.0.2:6667 6667
nat redirect_port tcp 192.168.0.3:80 80
```

Настроим переадресацию таким образом, чтобы весь трафик, приходящий на адрес "*192.1.1.1*", перенаправлялся в локальную сеть на адрес "*192.168.1.2* ", а трафик, приходящий на адрес "*192.1.1.2*", - в локальную сеть на адрес *"192.168.1.3"*.

```
nat redirect_address 192.168.1.2 192.1.1.1
nat redirect_address 192.168.1.3 192.1.1.2
```

Выполним настройку, при которой все пакеты TCP, исходящие из локальной сети на порт 80, перенаправлялись на прокси-сервер провайдера.

```
nat proxy_rule proto tcp port 80 server 123.1.1.1:3128
```

NAT и H.323 телефония

Абоненты и контроллеры (gatekeeper) – центры обработки вызовов внутри своей зоны используют несколько протоколов стека H.323. Нас интересуют два из них - RAS (registration, admission, status), используемый для регистрации абонентов на контроллере и для мониторинга статуса абонентов, и CS (call signalling), используемый абонентами для сигнализации в пределах одного звонка. Оба эти протокола описаны в стандарте H.225.0. Распространенные конфигурации систем включают в себя следующие примеры.

Абонент находится в частной сети, шлюз находится по реальному адресу, абонент осуществляет только исходящие звонки.

Для организации доступа абонента из частной сети к шлюзу можно воспользоваться параметром "*h323_destination"* с протоколом CS. Если шлюз принимает звонки на стандартный порт 1720, достаточно будет включить режим "*default_h323"*. Необходимо, чтобы абонент мог совершать исходящие звонки на шлюз.

Абонент находится в частной сети по адресу "*10.0.0.99*", шлюз - во внешней сети по адресу "*123.45.67.89*".

```
nat h323_destination cs 123.45.67.89 10.0.0.99
```

Абонент находится в частной сети по адресу "*10.0.0.99*", шлюз или несколько шлюзов – во внешней сети по неизвестным адресам.

```
nat default_h323
```

Несколько абонентов находятся в частной сети, шлюз находится по реальному адресу, осуществляются как исходящие, так и входящие звонки.

Для доступа шлюза к абонентам потребуется использовать настройку "*redirect_port"* с указанным протоколом CS, разными для разных абонентов "*alias"* адресами или портами (и прописать "*alias"* адреса и порты в конфигурации шлюза), а также явно указать адрес и порт шлюза и адреса абонентов (можно указать и порты абонентов). Необходимо, чтобы абоненты могли совершать исходящие звонки на шлюз и принимать звонки, входящие со шлюза.

Абоненты находятся в частной сети по адресам "*10.0.0.98*" и "*10.0.0.99*", шлюз - во внешней сети по адресу "*123.45.67.89*". "*Alias_address NAT"* пусть будет "*123.45.67.65*". В конфигурации шлюза надо будет указать адреса абонентов как "*123.45.67.65:1720*" и "*123.45.67.65:1721*" соответственно.

```
nat redirect_port cs 10.0.0.98:1720 1720 123.45.67.89
nat redirect_port cs 10.0.0.99:1720 1721 123.45.67.89
```

Title

Абонент из частной сети регистрируется на контроллере (gatekeeper) с реальным адресом и работает через контроллер. В этом случае достаточно задать параметр "*h323_destination ras"* и адрес контроллера. Если абоненты регистируются по стандартному для регистрации порту 1719, тогда можно просто включить режим "*default_h323"*.

Абонент находится в частной сети по адресу "*10.0.0.99*", а контроллер во внешней сети по адресу "*123.45.67.89*". Необходимо, чтобы абонент мог зарегистрироваться на этом контроллере, совершать и принимать через него звонки.

```
nat h323_destination ras 123.45.67.89 10.0.0.99
```

Некоторое число абонентов находится в частной сети, а контроллер во внешней сети по адресу "*123.45.67.89*" и нестандартному для RAS порту 1024. Необходимо, чтобы любой абонент мог зарегистрироваться на этом контроллере, совершать и принимать через него звонки.

```
nat h323_destination ras 123.45.67.89:1024
```

Абонент находится в частной сети по адресу "*10.0.0.99*", контроллер или несколько контроллеров – во внешней сети по неизвестным заранее адресам. Необходимо, чтобы абонент мог зарегистрироваться на любом контроллере, совершать и принимать через него звонки.

```
nat default_h323
```

Абонент с общедоступным адресом регистрируется на контроллере из частной сети. Потребуется применить параметр "*redirect_port"* с указанным протоколом RAS и указать в нем частный адрес и RAS-порт контроллера, чтобы абоненты из внешней сети смогли зарегистрироваться на этом контроллере. Для того, чтобы локальные абоненты тоже смогли работать с контроллером, нужно будет дополнительно задать параметр "*redirect_port*" с указанным протоколом CS и указать в нем локальный адрес и порт контроллера.

Абонент находится во внешней сети по адресу "*123.45.67.89*", а контроллер в частной сети по адресу "*10.0.0.99*". Необходимо, чтобы абонент мог зарегистрироваться на этом контроллере, совершать и принимать через него звонки. "*Alias_address NAT"* пусть будет "*123.45.67.65*". В конфигурации абонента адрес RAS контроллера должен будет выглядеть как "*123.45.67.65:1719*".

```
nat redirect_port ras 10.0.0.99:1719 1719 123.45.67.89
```

Локальный абонент находится во внешней сети по адресу "*123.45.67.89*", а контроллер в частной сети по адресу "*10.0.0.99*". Необходимо, чтобы абонент мог совершать и принимать через него звонки. "*Alias_address NAT"* пусть будет "*123.45.67.65*". В конфигурации абонента *CS* адрес контроллера должен будет выглядеть как "*123.45.67.65:1720*".

```
nat redirect_port s 10.0.0.99:1720 1720 123.45.67.89
```