Network Address Translation

Document revision 1.4 (Fri Apr 23 14:25:45 GMT 2004)
This document applies to V2.8

Table of Contents

General Information

Summary

Network Address Translation (NAT) provides ways for hiding local networks as well as to maintain public services on servers from these networks. Besides, through NAT additional applications like transparent proxy service can be made.

Quick Setup Guide

- Let us consider that we have a private network **192.168.0.0/24** and we want it to be able to use a single public IP address, which is assigned to interface **Public**. This can be done with masquerading:

```
[admin@MikroTik] ip firewall src-nat> add src-address=192.168.0.0/24
\... out-interface=Public action=masquerade
```

- Let us consider that we have a Web-Server in our private network **192.168.0.0/24** with IP address **192.168.0.2**. To redirect all HTTP traffic from the router's address (**10.5.8.104**) to the Web-Server, use the following command:

```
[admin@MikroTik] ip firewall dst-nat> add dst-address=10.5.8.104/32 dst-port=80 \
\... to-dst-address=192.168.0.2 protocol=tcp action=nat
```

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/ip firefall src-nat, /ip firewall dst-nat***
Standards and Technologies: ***IP***
Hardware usage: *Increases with rules and connections count*

Related Documents

- Package Management
- IP Addresses and ARP
- Routes, Equal Cost Multipath Routing, Policy Routing
- Firewall Filters

Description

NAT subdivision

Network Address Translation is subdivided into two separate facilities:

- Source NAT
  This type of NAT allows 'hiding' of private networks beyond the router. It alters forwarded IP packets' source addresses.
- Destination NAT
  This one is used for accessing public services on the local servers from outside the intranet. It can also help to accomplish some additional tasks like transparent proxying. Destination NAT alters forwarded IP packets' destination addresses.

Redirect and Masquerade

REDIRECT is similar to regular destination NAT in the same way as MASQUERADING is similar to source NAT - masquerading is source NAT, except you do not have to specify **to-src-address** - outgoing interface address is used automatically. The same is for REDIRECT - it is destination NAT where **to-dst-address** is not used - incoming interface address is used instead. So there is no use of specifying **to-src-address** for **src-nat** rules with **action=masquerade**, as well as no use of specifying **to-dst-address** for **dst-nat** rules with **action=redirect**. Note that **to-dst-port** is meaningful for REDIRECT rules - this is the port on which the service on router that will handle these requests is sitting (e.g. web proxy).

When packet is dst-natted (no matter - **action=nat** or **action=redirect**), dst address is changed. Information about translation of addresses (including original dst address) is kept in router's internal tables. Transparent web proxy working on router (when web requests get redirected to proxy port on router) can access this information from internal tables and get address of web server from them. If you are dst-natting to some different proxy server, it has no way to find web server's address from IP header (because dst address of IP packet that previously was address of web server has changed to address of proxy server). Starting from HTTP/1.1 there is special header in HTTP request which tells web server address, so proxy server can use it, instead of dst address of IP packet. If there is no such header (older HTTP version on client), proxy server can not determine web server address and therefore can not work.

It means, that it is impossible to correctly transparently redirect HTTP traffic from router to some other transparent-proxy box. Only correct way is to add transparent proxy on the router itself, and configure it so that your "real" proxy is parent-proxy. In this situation your "real" proxy does not have to be transparent any more, as proxy on router will be transparent and will forward proxy-style requests (according to standard; these requests include all necessary information about web server) to "real" proxy.

Notes

The **Connection Tracking** facility (**/ip firewall connection tracking**) must be enabled if you want to use NAT.

Source NAT

Description

Source NAT is a firewall function that can be used to 'hide' private networks behind one external IP address of the router. For example, it is useful, if you want to access the ISP's network and the Internet appearing as all requests coming from one single IP address given to you by the ISP. The Source NAT will change the source IP address and port of the packets originated from the private network to the external address of the router, when the packet is routed through it.

Source NAT helps to ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. It also conserves the number of global IP addresses required and it lets the whole network use a single IP address in its communication with the world.

Property Description

dst-address (*IP address*; default: **0.0.0.0/0:0-65535**) - destination IP address

src-address (*IP address*; default: **0.0.0.0/0:0-65535**) - source IP address

flow - flow mark to match. Only packets marked in the mangle facility would be matched

limit-time (*time*; default: **0**) - time interval, used in limit-count

protocol (*ah* | *all* | *ddp* | *egp* | *encap* | *esp* | *ggp* | *gre* | *hmp* | *icmp* | *idpr-cmtp* | *igmp* | *ipencap* | *ipip* | *iso-tp4* | *ospf* | *pup* | *rdp* | *rspf* | *st* | *tcp* | *udp* | *vmtp* | *xns-idp* | *xtp*; default: **any**) - protocol setting

- **all** - cannot be used, if you want to match packets by ports

icmp-options - ICMP options

content (*text*; default: **""**) - the text packets should contain in order to match the rule

comment (*text*; default: **""**) - a descriptive comment for the rule

connection (*text*; default: **""**) - connection mark to match. Only packets marked in the mangle facility would be matched

limit-burst (*integer*; default: **0**) - allowed burst for the limit-count during the limit-time

limit-count (*integer*; default: **0**) - specifies how many times to use the rule during the limit-time period

src-netmask (*IP address*) - source netmask in decimal form x.x.x.x

src-port (*integer*: 0..65535) - source port number or range

- **0** - means all ports from 0 to 65535

dst-netmask (*IP address*) - destination netmask in decimal form x.x.x.x

dst-port (*integer*: 0..65535) - destination port number or range

- **0** - means all ports from 0 to 65535

tos (*any* | *max-reliability* | *max-throughput* | *min-cost* | *min-delay* | *normal* | *integer*; default: **any**) - specifies a match for Type-of-Service field of an IP packet (see Firewall Filters manual for detailed description)

action (*accept* | *masquerade* | *nat*; default: **accept**) - action to undertake if a packed matched a particular src-nat rule, one of the:

- **accept** - accept the packet without undertaking any action, except for mangle. No more rules are processed in the relevant list/chain
- **masquerade** - use masquerading for the packet and substitute the source address:port of the packet with the ones of the router. In this case, the to-src-address argument value is not taken into account and it does not need to be specified, since the router's local address is used
- **nat** - perform Network Address Translation. The to-src-address should be specified (ignored when action=masquerade)

out-interface (*name*; default: **all**) - interface the packet is leaving the router from.

- **all** - may include the local loopback interface for packets with destination to the router

to-src-address (*IP address*; default: **0.0.0.0**) - source address to replace original source address with

to-src-port (*integer*: 0..65535) - source port to replace original source port with

Notes

The source nat can masquerade several private networks, and use individual **to-src-address** for each of them.

Masquerading chooses outgoing packets' source addresses according to the **preferred-address** property of the relevant route.

Example

To use masquerading, a source NAT rule with **action=masquerade** should be added to the **src-nat** rule set:

```
[admin@test_1] ip firewall src-nat> add src-address=192.168.0.0/24 \
\... out-interface=wlan1 action=masquerade
[admin@test_1] ip firewall src-nat> print
Flags: X - disabled, I - invalid, D - dynamic
  0   src-address=192.168.0.0/24:0-65535 dst-address=0.0.0.0/0:0-65535
      out-interface=wlan1 protocol=all icmp-options=any:any flow=""
      connection="" content="" limit-count=0 limit-burst=0 limit-time=0s
      action=masquerade to-src-address=0.0.0.0 to-src-port=0-65535

[admin@test_1] ip firewall src-nat>
```

If the packet matches the **masquerade** rule, then the router opens a connection to the destination, and sends out a modified packet with its own address and a port allocated for this connection. The router keeps

track about masqueraded connections and performs the "demasquerading" of packets, which arrive for the opened connections. For filtering purposes, you may want to specify the **to-src-ports** argument value, say, to 60000-65535

If you want to change the source address:port to specific adress:port, use the **action=nat** instead of **action=masquerade**:

```
[admin@test_1] ip firewall src-nat> add src-address=192.168.0.1/32 out-interface
=wlan1 action=nat to-src-address=1.1.1.1
[admin@test_1] ip firewall src-nat> print
Flags: X - disabled, I - invalid, D - dynamic
  0   src-address=192.168.0.1/32:0-65535 dst-address=0.0.0.0/0:0-65535
      out-interface=wlan1 protocol=all icmp-options=any:any flow=""
      connection="" content="" limit-count=0 limit-burst=0 limit-time=0s
      action=nat to-src-address=1.1.1.1 to-src-port=0-65535

[admin@test_1] ip firewall src-nat>
```

Here, the:

- **src-address** - can be IP host's address, for example, 192.168.0.1/32, or network address 192.168.0.0/24
- **to-src-address** - can be one address, or a range, say 10.0.0.217-10.0.0.219. The addresses should be added to the router's interface, or should be routed to it from the gateway router.

Destination NAT

Home menu level: ***/ip firewall dst-nat***

Description

Redirection and destination NAT should be used when you need to give access to services located on a private network from the outside world

Property Description

dst-address (*IP address*; default: **0.0.0.0/0:0-65535**) - destination IP address

src-address (*IP address*; default: **0.0.0.0/0:0-65535**) - source IP address

flow - flow mark to match. Only packets marked in the mangle facility would be matched

limit-time (*time*; default: **0**) - time interval, used in limit-count

protocol (*ah* | *all* | *ddp* | *egp* | *encap* | *esp* | *ggp* | *gre* | *hmp* | *icmp* | *idpr-cmtp* | *igmp* | *ipencap* | *ipip* | *iso-tp4* | *ospf* | *pup* | *rdp* | *rspf* | *st* | *tcp* | *udp* | *vmtp* | *xns-idp* | *xtp*; default: **any**) - protocol setting

- **all** - cannot be used, if you want to match packets by ports

icmp-options - ICMP options

content (*text*; default: "") - the text packets should contain in order to match the rule

comment (*text*; default: "") - a descriptive comment for the rule

connection (*text*; default: "") - connection mark to match. Only packets marked in the mangle facility would be matched

limit-burst (*integer*; default: **0**) - allowed burst for the limit-count during the limit-time

limit-count (*integer*; default: **0**) - specifies how many times to use the rule during the limit-time

period

src-netmask (*IP address*) - source netmask in decimal form x.x.x.x

src-port (*integer*: 0..65535) - source port number or range

- **0** - means all ports from 0 to 65535

dst-netmask (*IP address*) - destination netmask in decimal form x.x.x.x

dst-port (*integer*: 0..65535) - destination port number or range

- **0** - means all ports from 0 to 65535

tos (*any* | *max-reliability* | *max-throughput* | *min-cost* | *min-delay* | *normal* | *integer*; default: **any**) - specifies a match for Type-of-Service field of an IP packet (see Firewall Filters manual for detailed description)

action (*accept* | *redirect* | *nat*; default: **accept**) - action to undertake if a packed matched a particular dst-nat rule, one of the:

- **accept** - accept the packet without undertaking any action, except for mangle. No more rules are processed in the relevant list/chain
- **redirect** - redirects to the local address:port of the router. In this case, the to-dst-address argument value is not taken into account and it does not need to be specified, since the router's local address is used.
- **nat** - perform Network Address Translation. The to-dst-address should be specified (not required with action=redirect)

in-interface (*name*; default: **all**) - interface the packet has entered the router through

- **all** - may include the local loopback interface for packets with destination to the router

to-dst-address (*IP address*; default: **0.0.0.0**) - destination IP address to replace original with

to-dst-port (*integer*: 0..65535; default: **0-65535**) - destination port to replace original with

src-mac-address (*MAC address*; default: **00:00:00:00:00:00**) - host's MAC address the packet has been received from

Example

This example shows how to add a dst-NAT rule that gives access to the http server 192.168.0.4 on the local network via external address 10.0.0.217:

```
[admin@MikroTik] ip firewall dst-nat> add action=nat protocol=tcp \
\... dst-address=10.0.0.217/32:80 to-dst-address=192.168.0.4
[admin@MikroTik] ip firewall dst-nat> print
Flags: X - disabled, I - invalid, D - dynamic
  0   src-address=0.0.0.0/0:0-65535 in-interface=all
      dst-address=10.0.0.217/32:80 protocol=tcp icmp-options=any:any flow=""
      connection="" content="" src-mac-address=00:00:00:00:00:00
      limit-count=0 limit-burst=0 limit-time=0s action=nat
      to-dst-address=192.168.0.4 to-dst-port=0-65535

[admin@MikroTik] ip firewall dst-nat>
```