

nat command (Network Address Translation)



Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

[To the certification exam](#)

- [Description](#)
- [Parameters](#)
- [Examples](#)

Description

The "*nat*" command performs network address translation according to RFC1631. NAT allows to solve to some extent the problem of IPv4 address space exhausting. It means that several computers in the given LAN may connect to the Internet via the same public IP address. One IP address space is remapped into another by modifying network IP address information in the packets header during their transmission through the routing device.



NOTE

As it's known (rfc1918), some part of the IPv4 address space is reserved for using in so called private IP networks. Internet backbone routing protocols do not advertise these addresses, which allows to use the same addresses in different Internet segments. These addresses are used by ISP's and enterprises to build internal transport environment and/or to connect small subscriber communities.

```
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)
```

Syntax:



```


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

```

Parameters

Parameter	Description
-----------	-------------

local_acl \$NAME [public_addr] dhcp IFNAME] [-exclude \$DSTACL] [enable disable delete]	<p>Sets the real (public) IP-address which will be used for address translation. In order for the routing protocols to work normally, this address must be assigned to any physical interface of the router. Infinet Wireless router has at least two physical interfaces: Ethernet (eth) and radio (rf). Usually, the system is linked to ISP's backbone networks via radio interface and ISP's backbone is built using private networks.</p> <div data-bbox="352 365 1450 555" style="border: 1px solid #f9e79f; padding: 10px; margin: 10px 0;"> <p> NOTE</p> <p>Sometimes you can avoid public IP address assignment to physical interfaces at all. The procedure goal is to provide public IP address accessibility from Internet. But this may be done using static routing. The provider can describe the route to this IP address in such way to make the packets going to it reach your access unit. NAT-module will perform conversion before packet forwarding - it's enough that packets are entering into the router.</p> </div> <p>NAT module is designed in such a way so the original source and destination addresses are used (this is important when creating firewall rules, qm rules, ipstat analyzing). For example, when creating an IP Firewall rule, local addresses should be used for the private network. They will be shown in "ipstat" module also.</p> <p>This command also sets the name of an access list (ACL) of your private networks, which require network address translation. All packets with source addresses that are included into the "local_acl" list are considered as outgoing and are subject for translation. Exceptions are the packets going from "local_acl" to "local_acl", and packets going from "local_acl" to the router own addresses. All these packets same as the other packets are considered as incoming, if they are not reversed to the translated connections, will be passed through without being changed.</p> <ul style="list-style-type: none"> • "<i>\$NAME</i>" – name of local access list. • "<i>public_addr</i>" – a public IP-address that is used for an address translation. • "<i>dhcp IFNAME</i>" – an address received from the DHCP server. The interface through which DHCP issued the address is also need to be specified. • "<i>-exclude \$DSTACL</i>" – list of destination IP-addresses/networks that do not require address translation. • "<i>enable</i>" / "<i>disable</i>" / "<i>delete</i>" – allows to enable/disable/delete the rule.
maxlinks NUM	<p>Sets the maximum number of supported connections, 1000 are set by default. The system automatically observes all the connections and dynamically destroys all unnecessary connections according to their type and time of activity. However, when using different network scanners there is a possibility that current number of connections will increase enormously or until there is a free space in the RAM. This parameter helps to avoid this situation. In the case when the number of current connection exceeds the threshold set the system will put the warning into the system log and restrict new connection establishment until the situation becomes stable. When connections number will decrease the corresponding message will be put into the system log and a normal work will be resumed.</p>
"enable"	Enables NAT-module to start NAT according to specified rules.
"disable"	Disables NAT, but keeps all previously entered rules.
same_ports [yes/no]	<p>If enabled, forces NAT-module to keep ports numbers in the modified packets as they are. If it is impossible then arbitrary port numbers will be used. By default is enable.</p> <ul style="list-style-type: none"> • "<i>yes</i>" / "<i>no</i>" – enable/disable the function.
verbose [yes/no]	Enables/Disables diagnostic mode and printing information about modified packets into system log.
proxy_only [yes/no]	If enabled, NAT-module only forwards packet according to " <i>proxy_rule</i> " commands. Common NAT not performed.
stat	Shows NAT statistics.
ignore_incoming [yes/no]	Enables/Disables ignoring unknown incoming connections.
skinny_port port	<p>Sets the TCP port for the Skinny protocol. Skinny is used by Cisco IP-phones for connection to Cisco Call Managers. The "<i>Skinny aliasing</i>" command won't be performed, if no data is entered. Default port for Skinny is 2000.</p>
default_h323 [yes/no]	<p>Includes address modification according with H.323 stack for outgoing connections. Affects all incoming UDP packets destined for port 1719 and incoming TCP connections for port 1720. By default is disabled.</p> <div data-bbox="352 1812 1450 1928" style="border: 1px solid #f9e79f; padding: 10px; margin: 10px 0;"> <p> CAUTION</p> <p>Do not enable this option unless it used for IP telephony applications, otherwise the NAT performance will be hindered.</p> </div>

h323_destination ras cs remote_addr: remote_port] [local_addr: local_port]]	<p>Enables to specify H.323 elements using in the external network more specifically. For a detailed description see the section "NAT and H.323 telephony".</p> <ul style="list-style-type: none"> • "ras cs" – H.323 stack layer specified for processing. • "remote_addr" – address of external network, its connections will be processed. • "remote_port" – port value, its outgoing connections will be processed. If port is not specified then 1719 is used for RAS and 1720 for CS. • "local_addr" – LAN host address, its outgoing connections will be processed. If address not specified then any port connections will be processed. • "local_port" – port for processing outgoing messages. If port is not specified, all connections from all ports are processed.
del rule_number	Deletes the rule with selected number. The "config show" command allows to display all numbers.
Packet redirection	
redirect_port proto local_addr: local_port_range [public_addr:] public_port_range [remote_addr: remote_port_range]]	<p>This parameter is dedicated for creating redirection rules. NAT disadvantage is that local hosts are not accessible from the Internet. Local hosts can establish outgoing connections but cannot serve incoming. This hinders starting Internet applications on local hosts. Simple solution is to redirect incoming traffic on specified ports to local hosts. Multiple command execution with different arguments allowed. Rules are numbered when the "config show" command is performed. It allows to delete rules using the "nat del XX" command where "XX" is a sequential number.</p> <ul style="list-style-type: none"> • "proto" – specifies the protocol value, may be "tcp", "udp", "ras" or "cs". In case of "ras" or "cs" value, the address modification is performed according to H.323. • "local_addr:local_port_range" – an IP-address and a port of the local host which traffic will be redirected to. The second version of the command can be used: "local_addr_1:local_port_range[, local_addr_2:local_port_range, ...]", it allows to perform incoming packets cyclical forwarding to several addresses (LSNAT) and helps to distribute the load between them. • "[public_addr:]public_port_range" – a public IP-address and a port of the device. In case of using several pairs "public address - private network" simultaneous it is recommended to specify the exact public address. • "[remote_addr:remote_port_range]" – specified for more exact definition of incoming packets (packets only from specified source and port will be allowed). If "remote_port_range" is not specified then its range should coincide with range of "public_port_range". <div style="border: 1px solid #f9e79f; padding: 10px; margin-top: 10px;"> <p> NOTE</p> <p>The port ranges "local_port_range" and "public_port_range" should be the same size.</p> </div>
redirect_address local_addr[,...] public_addr	Redirects all incoming traffic directed to "public_addr" to "local_addr". If several "local_addr" addresses specified then redirection will be done in round-robin way. Address redirection makes sense when there are several IP-addresses on the same host. In this case NAT can assign to every LAN client its own external IP-address. Then NAT transforms outgoing packets, changing IP-addresses to public external IP-addresses.
redirect_proto proto local_addr [public_addr [remote_addr]]	Redirects all the incoming packets with specified protocol "proto" to the host with address "local_addr". If the "remote_addr" parameter is specified, then only packets from this address are processed.
proxy_rule [type encode_ip_hdr encode e_tcp_stream] [port xxxx] [server [a.b.c.d]: yyyy] [proto tcp udp] [src <addr>/mask]] [dst <addr>/mask]]	<p>Performs redirection of outgoing packets. TCP packets outgoing from LAN to any address with specified port, redirected to specified server and port. Optionally initial destination address may be included into the packet using several ways. The parameter consists of word pairs: key parameters and its value.</p> <ul style="list-style-type: none"> • "type" – if transparent gateway requires information of initial address and an access port of a new server, then it may be done in two following ways: <ul style="list-style-type: none"> • "encode_ip_hdr" – original address and port are transmitted in extended IP header fields (IP option). • "encode_tcp_stream" – original port and address are transmitted in a packet before data start in format "DEST IP port". • "port xxxx" – only packets sent to specified port are processed. • "[server [a.b.c.d]:yyyy]" – mandatory parameter. Specifies server address and port for packet redirection. If port not specified then original destination port will be used. • "[proto tcp udp]" – only packets with specified protocol will be processed. • "[src <addr>/mask]" и "[dst <addr>/mask]" – specifies source/destination network (subnetwork) for packet redirection.

Examples

By using the *"ifconfig"* command set the public IP-address *"123.1.1.1/32"* for the *"rf5.0"* interface. Enable a dynamic routing for public IP-address by entering the *"rip start"* command.

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

Create an access list with *"192.168.1.0/24"* as the only network (our local network) and set the *"123.1.1.1"* IP-address as public for this network.

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

Or use the address received by the DHCP protocol as a public address. DHCP server has issued an IP-address through the *"eth0"* interface.

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

Allow the NAT module to perform the address translation in accordance with established rules.

```
nat enable
```

In following example, all incoming TCP connections to the 7777 port of this router are redirected to the host with the *"192.168.1.5"* IP-adress, port 23 (telnet).

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

All incoming TCP packets with *"public_port_range"* 3300-3399 and destination address *"123.1.1.2"* are redirected to the *"192.168.1.4"* address. Port mapping is *"1 to 1"*, i.e. 3300->2300, 3301->2301.

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

The IRC-server is running on the client A and the WEB-server is running on the client B. Then in order to make it work, connections accepting on ports 6667(irc) and 80(web), should be redirected to the appropriate hosts.

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

NAT settings in this example provide the redirection of all traffic incoming to the *"192.1.1.1"* IP-address to the LAN address *"192.168.1.2"*, and traffic incoming to *"192.1.1.2"* is redirected to *"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
```

All outgoing LAN TCP packets destined for port 80 will be redirected to provider proxy server.

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

NAT and H.323 telephony

Subscribers and gatekeepers use several H.323 protocols. We are interested in two. RAS (registration, admission, status) used for subscriber registration on the gatekeeper and to monitor subscriber status. CS (call signaling) used by subscribers for signaling established for a specific call. Both these protocols described H. 225.0 standard. Well known system configurations includes the following examples.

A subscriber resides in a LAN, and a gateway has a public IP-address. A subscriber makes outgoing calls only.

Use the "*h323_destination*" parameter to provide for a subscriber from a local network an access to the gateway by the CS protocol. If the gateway accepts calls incoming to the 1720 well-known port, it is enough to turn the "*default_h323*" mode on.

The subscriber resides in the LAN and has the "*10.0.0.99*" IP-address, the gateway has the "*123.45.67.89*" IP-address and resides in the Internet. Allow subscriber outgoing calls to the gateway by using following command:

```
nat h323_destination cs 123.45.67.89 10.0.0.99
```

The subscriber resides in the LAN and has the "*10.0.0.99*" IP-address, a gateway or several gateways are in the Internet with unknown addresses. Allow subscriber outgoing calls to the gateway by using following command:

```
nat default_h323
```

Several subscribers reside in a LAN, a gateway has a public IP-address, calls are both incoming and outgoing.

For access from the gateway to the subscribers the "*redirect_port*" command should be used with the "*cs*" protocol specified, different alias addresses or ports. Directly specify gateway port and address (subscriber ports may be specified as well).

Subscribers reside in the LAN having addresses "*10.0.0.98*" and "*10.0.0.99*", gateway resides in the Internet having address "*123.45.67.89*". NAT "*alias_address*" is "*123.45.67.65*". Allow subscribers to make outgoing calls to the gateway and to receive incoming calls from the gateway by using following command:

```
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
```

A subscriber resides in a LAN, gets registered on the gatekeeper with public IP-address and works via gatekeeper.

To specify the "*h323_destination ras*" command and the gatekeeper address will be enough in this case. The "*default_h323*" mode can be enabled if subscribers make registration on the standard port 1719.

A subscriber resides in the LAN having the "*10.0.0.99*" IP-address, gatekeeper resides in the Internet having the "*123.45.67.89*" address. Allow the subscriber to get registered on the gatekeeper, for making and receiving calls, by using following command:

```
nat h323_destination ras 123.45.67.89 10.0.0.99
```

Several subscribers reside in a LAN, the gatekeeper in the Internet has the "*123.45.67.89*" IP-address and non-RAS standard port 1024. Allow any subscriber to get registered on the gatekeeper for making and receiving calls, by using following command:

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

A subscriber resides in a LAN having the "*10.0.0.99*" IP-address and a gatekeeper or several gatekeepers reside in the Internet with unknown addresses. Allow the subscriber to get registered on unknown addresses, by using following command:

```
nat default_h323
```

A subscriber with the private IP-address gets registered on the gatekeeper from LAN.

The "*redirect_port*" rule with ras protocol, its private IP-address and a gatekeeper RAS port must be specified to enable subscribers from the Internet to be registered on the gatekeeper. Since static subscribers also should work with the gatekeeper, the "*redirect_port*" rule with protocol CS, a private gatekeeper IP-address and its port should be specified as well.

A subscriber resides in the Internet having the "*123.45.67.89*" IP-address, and the gatekeeper resides in a LAN having the "*10.0.0.99*" address. NAT "*alias_address*" is "*123.45.67.65*". Allow subscriber registered on this gatekeeper for making and receiving calls, by using following command:

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

RAS gatekeeper address is "*123.45.67.65:1719*".

Static subscriber resides in the Internet having the "*123.45.67.89*" IP-address and the gatekeeper resides in a LAN having the "*10.0.0.99*" address. NAT "*alias_address*" is "*123.45.67.65*". Allow subscriber registered on this gatekeeper for making and receiving calls, by using following command:

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

In the subscriber configuration the gatekeeper IP-address should be "*123.45.67.65:1720*".