# New NAT

bintec Dm788-I

## Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

# Table of Contents

# I Related Documents

bintec Dm720-I NAT Feature

bintec Dm735-I NAPT Facility

bintec Dm755-I Dynamic NAT

bintec Dm786-I AFS

# Chapter 1 Introduction

## 1.1 NAT

Depletion of IP address space and scaling in routing are two of the key problems the Internet has to face. Network Address Translation (NAT) is a feature that translates the private (local) addresses an organization uses into public addresses, creating a globally routable address space that is accessible from the Internet. NAT also allows organizations to launch readdressing strategies where changes in the local IP networks are minimum.

NAT has several applications. The following scenarios are just a few examples:

- If you want to connect to the Internet, but not all your hosts have globally unique IP addresses (allowed). NAT is configured on the router at the border of a stub domain (local network) and a public domain such as the Internet (outside network). The NAT translates the inside local addresses to globally unique IP addresses before sending packets to the outside network.
- An organization requires IP connectivity between remote offices. The remote offices have private or internal IP networks that do not comply with the addressing plan (since the routing tables through which connectivity is carried out between them are large or unmanageable). In this case, configuring NAT in the border router of each office would be enough to carry out the translation between office networks and global networks (as these now comply with the addressing plan).
- You must change your internal addresses. Since changing them can take a considerable amount of time and effort, you can translate them using NAT.

One of NAT's main advantages is that it can be configured without having to change the hosts or routers that will not run NAT. The disadvantages of NAT appear when large numbers of hosts require NAT simultaneously, or when the network applications exchange source or destination IP address references. Since these applications do not work if the information is sent through a NAT router in transparent mode, the NAT router must analyze the application's data packet and change the references to local IP addresses.

A router configured with NAT has at least one local interface (in contact with the local network) and one global interface (in contact with the global network). In a typical environment, NAT is configured at the exit router between a stub domain and backbone. When a packet is leaving the domain, NAT translates the locally significant source address into a globally unique address. When the packet is entering the domain, NAT translates the globally unique address into a local address.

A router configured with NAT must not advertise local networks externally. However, global routing can be advertised through local interfaces.

As previously mentioned, the term *local* refers to networks owned by an organization that must be translated. Inside the domain, hosts will have addresses in one address space whereas, externally, they will appear to have addresses in another. The first address space is known as the *local* address space, while the second is referred to as the *global* address space.

NAT can be executed both at source and at destination.

- NAT at source. The NAT router replaces the local source IP for a new global IP. The reverse operation is carried out over the destination IP for packets that go through the router in the opposite direction.
- NAT at destination. The NAT router replaces the global destination IP with a new local destination IP. This is mainly used to make devices or subnets visible from the Internet. The reverse operation is carried out over the source IP for those packets going through the router in the opposite direction.

**Types of NAT:**

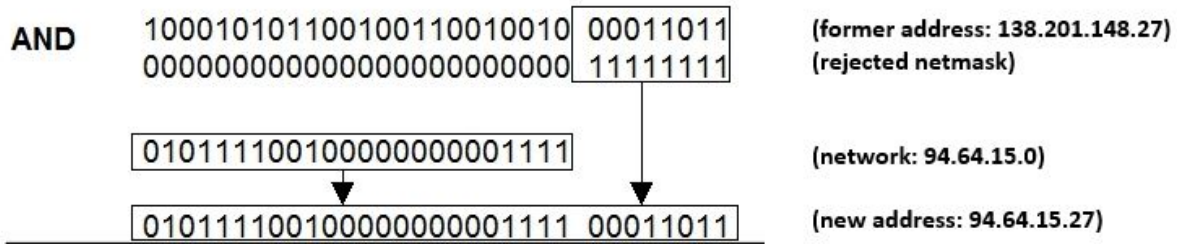
The AFS system supports two types of NAT, both at source and at destination:

**Static NAT**

- In static NAT, the translations are added to the NAT table as soon as the rule is configured in the system, and are kept until they are deleted from the configuration. These translations can only affect the packet IP addresses or the TCP/UDP ports.

  **Example**: translating from one IP network to another:

- Translate all the 138.201.148.0 local network addresses in the 94.64.15.0 global network, netmask is 255.255.255.0 for both.




**Example**: Visible port

- Translate IP packets with global destination IP address 1.1.1.1 and TCP port 23 into packets with local IP destination address 172.24.100.130 and TCP port 23.

**Dynamic NAT**

- In dynamic NAT, translations don't appear in the NAT table until the router receives traffic requiring translation. Dynamic translations have a certain lifespan, and are then deleted from the translation table.

  There are two types of dynamic NAT, overload and no-overload.

  In overload mode, the same local IP can be mapped to various global IPs changing the associated TCP/UDP port. This type of NAT is also known as PAT.

  **Example:**

- NAT rule: masquerade the 138.201.0.0 global network addresses after the router's external global interface address.
- For each outgoing packet, the source address is replaced by the outside interface address generated by the NAT router and the source port is exchanged for an unused NAT port.
- If the destination of the incoming packets is the NAT router's outside interface address and the destination port corresponds to a NAT port that has been already assigned, the address and port are exchanged for the corresponding local address and local port.

  In no-overload mode, there is a one-to-one correspondence between a local IP and a global IP. However, unlike what happens with static NAT, this correspondence is decided when executing and where necessary.

  **Example**:

- Dynamically translate all the 138.201.0.0 local network addresses with mask 255.255.0.0 into 278.201.112.0 global network addresses with mask 255.255.255.0.

The bintec OS supported these three types of NAT through three different menus: one for port NAT (please see manual *bintec Dm735-I NAPT Facility*) another for dynamic NAT (please see manual *bintec Dm755-I Dynamic NAT*) and one for static NAT (please see *bintec Dm720-I NAT Feature*). This new NAT replaces these three NAT subsystems and allows all three types of NAT to be executed from a single menu.

To configure this new NAT, you need to enable the AFS feature (please see manual *bintec Dm786-I AFS*). Since the new NAT rules are now checked once per session (instead of per packet) the AFS system must be active to carry out session tracking.

# Chapter 2 Configuring NAT

## 2.1 Configuring NAT

To configure NAT, the AFS system must be enabled (see manual *bintec Dm786-I AFS*). Once enabled, access the configuration through the IP configuration menu.

*Syntax:*

```
Config>protocol ip
-- Internet protocol user configuration --
IP config>nat
NAT config>
```

If you want to configure a specific VRF, first access the VRF menu through the IP protocol configuration menu and subsequently enter NAT. E.g. to configure the NAT system in the bintec VRF:

*Example:*

```
Config>protocol ip
-- Internet protocol user configuration --
IP config>vrf bintec
IP vrf config>nat
NAT config>
```

The NAT system configuration is identical for both the main VRF and the secondary VRFs. The following explanation applies to both.

The options presented in the NAT system configuration menu are as follows:

```
NAT config>?
  no          Negate a command or set its defaults
  pool        Define an ip pool
  rule        Configure an afs rule
  exit
NAT config>
```

### 2.1.1 [NO] POOL

This command defines a pool of IP addresses that can be later used to execute dynamic NAT.

*Syntax:*

```
NAT config>POOL <pool-id> ip <ip-min> <ip-max>
NAT config>
```

| | |
|---|---|
| *pool-id* | Pool identifier. This can be subsequently associated to a NAT rule to execute dynamic NAT. |
| *ip-min* | Lowest IP in the pool. |
| *ip-max* | Highest IP in the pool. |

*Example:*

The following configuration defines a pool with identifier 1 and is made up of three IP addresses: 1.1.1.1, 1.1.1.2 and 1.1.1.3.

```
NAT config >pool 1 ip 1.1.1.1 1.1.1.3
NAT config>
```

### 2.1.2 [NO] RULE

Configures the NAT rules. A rule is an action that is executed if the packet matches the selection criteria associated to said rule. This criteria can be both an input/output interface and an access list.

It's important to bear in mind that rules are run in the order in which they are configured. When a packet matches an input/output NAT rule, the rest of the input/output rules are not processed. The transformation executed over the IP packet is the one corresponding to the matching rule.

*Syntax:*

```
NAT config>RULE <rule-id> <position> [<interface>] [list <list>] <nat-type>
NAT config>
```

| | | |
|---|---|---|
| *rule-id* | | Rule number, accepts values ranging from 1 to 10000. |
| *position* | | Supports one of these three positions. |
| | *out* | The rule is checked just before the packet exits the router through any interface. |
| | *in* | The rule is checked just after receiving a packet through any interface. |
| *interface* | | Specifies an interface for the rule. If the rule is input only, it executes if the packet enters through said interface and if the rule is output only, it executes if the packet exits through said interface. |
| *list* | | Specifies an access list. The rule is only applied if the IP packet matches said access list. |
| *nat-type* | | Defines the type of NAT. |
| | *static* | Static NAT. The static rules are bidirectional, i.e. configuring a rule at the output internally configures the opposite rule at the input. Due to its bidirectional nature, and to avoid confusions, static rules can only be configured at the output. |
| | *dynamic* | Dynamic NAT. |
| | *dynamic overload* | Dynamic NAT with address overload, also known as PAT. Two or more local IP addresses can be mapped to the same global IP address. |

After defining where to apply the rule and the type of NAT, you need to define how the translation is going to be executed. You can also configure a description of said rule (and disable it). This will be explained further on.

The translation syntax changes depending on whether you're dealing with dynamic or static NAT.

*Syntax:*

Rules for dynamic NAT:

```
NAT config>RULE <rule-id> TRANSLATION [source|destination]
   address          IP address or IP network
   gre-id           Define a gre id range
   http             Http specific NAT options
   icmp-id          Define an icmp id range
   interface        Use an interface unnumbered address to do nat
   pool             Use a nat pool
   tcp              Define a tcp port range
   udp              Define an udp port range
NAT config>RULE <rule-id> TRANSLATION [type]
  fullcone-pat      Full-cone pat behaviour
  symmetric-pat     Symmetric pat behaviour
NAT config>
```

| | |
|---|---|
| *rule-id* | Rule number, accepts values ranging from 1 to 10000. |
| *source* | Indicates that NAT must be executed over the source IP/port. |
| *destination* | Indicates that NAT must be executed over the destination IP/port. |
| *address* | Specifies an IP or a global IP network to which the packet's local address can be mapped (if said packet matches the rule selection criteria). |
| *gre-id* | Specifies a range of global GRE identifiers used to map the local GRE identifiers. |
| *http force-identity-encoding* | The outgoing http petitions are modified so that they only accept responses without any type of compression. This is useful if you wish to filter web traffic by content since, if this is compressed, content is inaccessible. |
| *icmp-id* | Specifies a range of global ICMP identifiers that are used to map the local ICMP identifiers. |
| *interface* | The global address used to execute the translation is the IP address assigned to the specified interface. |
| *pool* | Defines a pool of global addresses to use in the translation. |

| | |
|---|---|
| *tcp* | Specifies a range of global TCP ports used to map the local TCP ports. |
| *udp* | Specifies a range of global UDP ports used to map the local UDP ports. |
| *type* | Determines the type of NAT to be applied to the rule. If this parameter is not configured, the default NAT applied to the rule is "symmetric-pat". |
| *fullcone-pat* | Executes a full cone NAT, where the local IP address and port are mapped to a global IP address and port. All the inbound packets to this global address and port are mapped to the local host. |
| *symmetric-pat* | This kind of NAT translates the local IP address and port to a global IP address and port but the destination is fixed. Packets are only routed to the local host if the source address and port match the original destination. |

*Syntax*

Rules for static NAT:

```
NAT config>RULE <rule-id> TRANSLATION SOURCE
                <local-ip> <global-ip>
               network <local-net> <global-net> <mask>
               tcp          TCP visible port
               udp          UDP visible port
NAT config>
```

*<rule-id>*

Rule number, accepts values ranging from 1 to 10000.

*<local-ip> <global-ip>*

Specifies the source local IP address that is changed for the global IP which is specified next. As a global IP you can specify an interface, therefore taking the main IP for said interface as global IP.

*network <local-network> <global-network> <network-mask>*

Specifies a local IP network. All IP addresses with said local network as source are mapped to the network specified through the global-network parameter.

*tcp <local-ip> <local-port> <global-ip> <global-port>*

Indicates that a TCP port and a local IP must be mapped to a specified TCP port and global IP. This command is used to configure visible TCP ports. As global IP, you can specify an interface, taking the main IP for said interface as the global IP.

*udp <local-ip> <local-port> <global-ip> <global-port>*

Indicates that a UDP port and a local IP must be mapped to a specified UDP port and global IP. This command is used to configure visible UDP ports. As global IP, you can specify an interface, taking the main IP for said interface as the global IP.

*Example 1:*

A NAT rule is configured to map the local address for all packets that exit through the PPP1 interface (and match access list 1) to the global address assigned to the PPP1 interface. This type of NAT is dynamic overload (PAT).

```
NAT config>
    rule 1 out ppp1 list 1 dynamic overload
    rule 1 translation source interface ppp1
NAT config>
```

*Example 2:*

In the above example, we want to create a visible port for the telnet, so the TCP connections directed to the 2323 global IP port are mapped to the local IP 172.24.100.131 port 23.

```
NAT config>
    rule 1 out ppp1 static
    rule 1 translation source tcp 172.24.100.131 23 ppp1 2323
NAT config>
```

*Example 3:*

We want to statically map local IP address 1.1.1.1 to 2.2.2.2.

```
NAT config>
```

```
    rule 1 out static
    rule 1 translation source 1.1.1.1 2.2.2.2
NAT config>
```

*Example 4:*

We want to translate local IP addresses into the global address pool made up of 4 addresses (1.1.1.1, 1.1.1.2, 1.1.1.3 and 1.1.1.4) for all packets that exit through interface ppp1 and match access list 1.

This type of NAT is dynamic, but port translation is not executed (only IP address translation is carried out).

```
NAT config>
    pool 1 ip 1.1.1.1 1.1.1.4
;
    rule 6 out ppp1 list 1 dynamic
    rule 6 translation source pool 1
NAT config>
```

You can also configure a description for the rule (and disable it), as described earlier through the description and shutdown commands:

```
NAT config>rule 1 ?
  description    Description of this rule
  shutdown       Disable this rule
  translation    NAT translation configuration
```

*Example:*

```
NAT config>rule 1 description MAP_PPP1
NAT config>rule 6 shutdown
```

*Example 5:*

In this example, we configure a full cone NAT where the local host can be accessed through the global IP and port mapped. In this case, the global IP address is going to be the 7.7.7.7, and the global interface is the WAN. All the packets with IP 7.7.7.7 and the global open port as destination are mapped to the local host. The configuration is as follows:

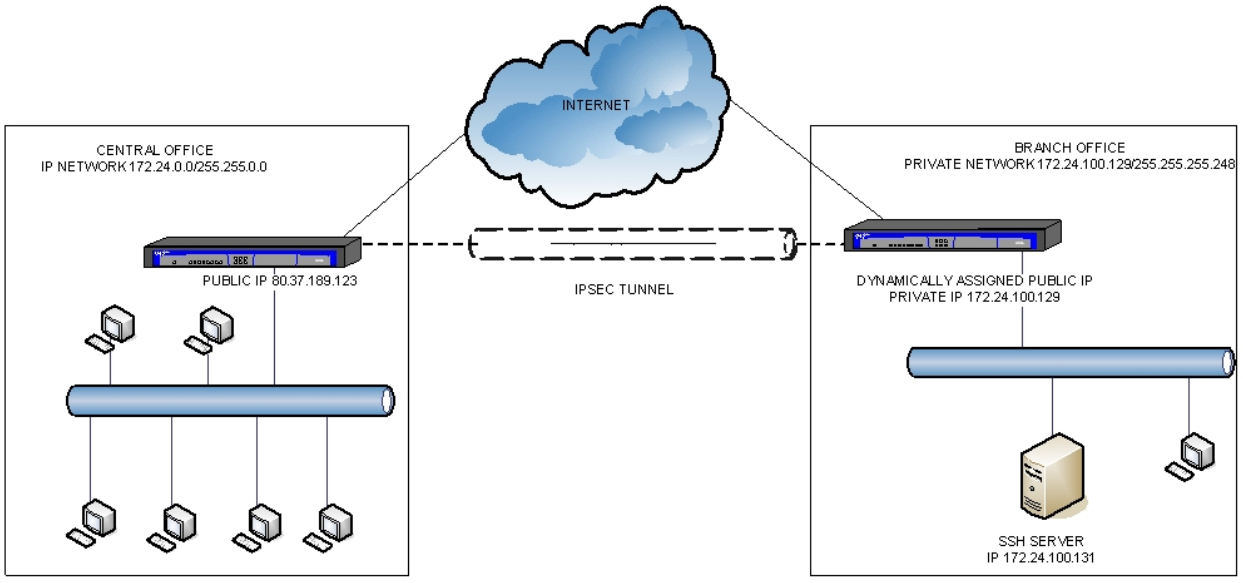
```
NAT config>rule 1 out ethernet0/1 dynamic overload
NAT config>rule 1 translation source address 7.7.7.7
NAT config>rule 1 translation type fullcone-pat
```

# Chapter 3 Configuration Examples

## 3.1 Remote office connected through IPSEC

This example describes a typical scenario: a remote office wants to stay connected with the central headquarters and to have its own Internet access. A PPP interface over ATM is used as the outgoing interface.

The network for the headquarter office is 172.24.0.0 255.255.0.0 and the remote branch has IP subnet 172.24.100.128/255.255.255.248. The office router must encapsulate the IP packets with the central headquarters network as destination in an IPSEC tunnel, without executing any type of NAT. Packets with any other destination must be subjected to NAT dynamic overload (PAT). This way, the traffic between the remote and central office is encapsulated in IPSEC (creating a VPN) and the rest of the traffic directed to the Internet does not pass through the main headquarters (thus saving bandwidth).




The following sections describe how to configure the office router.

*PPP:*

The output interface for the office is an ATM interface over which PPP is mounted. The IP address is not fixed, it's assigned by the carrier. This PPP interface is used as the default route.

```
   add device ppp 1
   network ethernet0/0
; -- Ethernet Interface User Configuration --
      ip address 172.24.100.129 255.255.255.248
   exit
;
   network atm2/0
; -- ATM interface configuration --
      aal-connection 1 pvc 8 32
;
      pvc 8 32 default
;
   exit
;
   network atm2/0.1
; -- ATM subinterface configuration --
      aal-connection-requested 1 default
;
   exit
;
;
   network ppp1
; -- Generic PPP User Configuration --
      ip address unnumbered
;
```

```
      ppp
; -- PPP Configuration --
         ipcp local address assigned
      exit
;
      base-interface
; -- Base Interface Configuration --
         base-interface atm2/0.1 link
;
      exit
;
      pppoe
; -- PPPoE User Configuration --
         enable pppoe
      exit
;
   exit
;
   protocol ip
; -- Internet protocol user configuration --
      internal-ip-address 172.24.100.129
;
      route 0.0.0.0 0.0.0.0 ppp1
;
      classless
   exit
```

*IPSEC:*

An IPSEC tunnel is configured. Its source address must be the public IP assigned to the PPP1 interface and its destination address the public IP address for the access router located at the main headquarters. An access list is created to encapsulate packets in the IPSEC tunnel with source being IP network 172.24.100.128/255.255.255.248 and destination 172.24.0.0/255.255.0.0 (or vice versa).

```
   feature access-lists
; -- Access Lists user configuration --
      access-list 101
         description "ipsec access-list"
         entry 1 default
         entry 1 permit
         entry 1 source address 172.24.100.128 255.255.255.248
         entry 1 destination address 172.24.0.0 255.255.0.0
;
      exit
   exit
;
   protocol ip
; -- Internet protocol user configuration --
;
      ipsec
; -- IPSec user configuration --
         enable
         assign-access-list 101
;
         template 2 dynamic esp tdes md5
         template 2 source-address ppp1
         template 2 destination-address 80.37.189.123
         template 2 life duration seconds 23h50m
         template 2 ipcomp lzs
         template 2 mtu-default 1100
;
         template 3 isakmp tdes sha1
         template 3 destination-address 80.37.189.123
         template 3 life duration seconds 1d
         template 3 ike mode aggressive
         template 3 ike idtype keyid
         template 3 ike natt-version rfc
         template 3 keepalive dpd
```

```
;
         map-template 101 2
         key preshared ip 80.37.189.123 ciphered 0x1E223C9C4D1703F065040FD4F9D
         advanced dpd always-send
         qos-pre-classify
      exit
;
   exit
;
```

*NAT:*

The PPP1 interface reaches the Internet and executes PAT with the interface's public IP address. To make FTPs possible, the corresponding ALG is loaded in the AFS system.

As the traffic is encapsulated in IPSEC, NAT should not be executed. The exclusion of traffic that is encrypted by IPSEC from the NAT subsystem, is automatically carried out by the AFS system.

```
   feature afs
      alg ftp port 21
;
      enable
   exit
   protocol ip
      nat
         rule 1 out ppp1 dynamic overload
         rule 1 translation source interface ppp1
         rule 1 description "NAT to everything but IPSEC"
      exit
   exit
```

We want to be able to access the SSH server from the Internet. The server is located in the office with internal IP 172.24.100.131, so a static NAT translation is configured to enable port 22:

```
rule 2 out ppp1 static
rule 2 translation source tcp 172.24.100.131 22 ppp1 22
```

There are IP telephones with SIP in the office, and we want to prioritize voice traffic over data. To do this, a route-map is configured that marks the RTP flows with a given tos. An access list is also configured to prioritize said tos and the port used for SIP signaling (UDP 5060).

*MARKED:*

```
   feature access-lists
; -- Access Lists user configuration --
      access-list 5000
         entry 1 permit
         entry 1 rtp
;
         entry 2 deny
      exit
   exit
   feature route-map
; -- Route maps user configuration --
      route-map "mark-rtp"
         entry 1 default
         entry 1 permit
         entry 1 set ip tos-octet 20
;
      exit
;
   exit
   network ethernet0/0
      ip policy route-map rtp
   exit
```

*BRS:*

```
     access-list 103
         description "voip brs class"
;
```

```
         entry 5 default
         entry 5 permit
         entry 5 tos-octet 20
;
         entry 1 default
         entry 1 permit
         entry 1 destination port-range 5060 5060
         entry 1 protocol udp
;
         entry 2 default
         entry 2 permit
         entry 2 source port-range 5060 5060
         entry 2 protocol udp
;
      exit
   feature bandwidth-reservation
; -- Bandwidth Reservation user configuration --
      network ppp1
         enable
         class local 5
;
         class default 95
;
         class voip 100 real-time
;
         access-list 103 voip
;
      exit
;
   exit
;
```

## 3.2 DYNAMIC NAT

A company has five public IP addresses assigned: 80.1.1.1, 80.1.1.2, 80.1.1.3, 80.1.1.4 and 80.1.1.5. We want to use the first of these to make internal IP 172.24.1.1 visible and the other four to carry out dynamic NAT addressing over the rest of the internal IPs. We don't want to execute translation on the port number (PAT).

Internet output is carried out through a PPP interface, PPP1.

*Configuration:*

The following configuration refers to NAT and AFS only.

Two NAT rules are defined, one static to map IP address 172.24.1.1 to 80.1.1.1 and another, dynamic, to map the rest of the IP addresses to the address pool.

Please bear in mind that, in the access list associated to the dynamic NAT feature, an entry has been added so that visible IP address 172.24.1.1 is not subjected to NAT. Since the dynamic NAT rule is configured before the static rule, not configuring this entry would mean packets with IP source 172.24.1.1 would match NAT rule 1 (forcing dynamic NAT to be carried out over them).

```
   feature afs
      alg ftp port 21
;
      enable
   exit
   feature access-lists
; -- Access Lists user configuration --
      access-list 102
         entry 1 default
         entry 1 deny
         entry 1 source address 172.24.1.1 255.255.255.255
;
          entry 2 default
         entry 2 permit
          entry 2 source address 172.24.0.0 255.255.0.0
      exit
```

```
   exit
   protocol ip
      nat
         pool 1 ip 80.1.1.2 80.1.1.5
;
         rule 1 out ppp1 list 102 dynamic
         rule 1 translation source pool 1
;
         rule 2 out ppp1 static
         rule 2 translation source 172.24.1.1 80.1.1.1
      exit
   exit
```