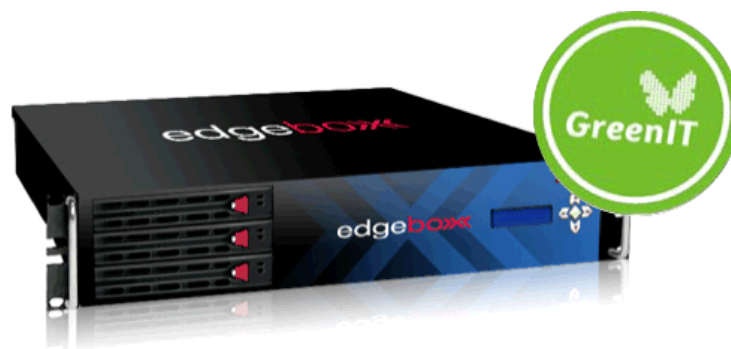


Dramatically simplifying voice and data networking



# edgeboxx

## HOW-TO GUIDE

Configuring NAT



## Table of Contents

Introduction to NAT .....	3
NAT .....	3
Port forwarding (NAPT) .....	4

# Introduction to NAT

This document will give a brief introduction to NAT – Network Address Translation – and NAPT – Network Address and Port Translation. Then it will focus on what edgeBOX allows its users to do with this technology.

In order to associate a network packet with an IP (Internet Protocol) communication connection, a tuple of five attributes is needed. This tuple contains:

1. source IP address
2. source port
3. destination IP address
4. destination port
5. protocol

NAT is the ability to change 1. and/or 3. attributes of a connection and NAPT is the ability **additionally** change 2. and/or 4. Therefore NAT applies **exclusively** at the network layer (OSI layer 3).

This will allow the creation of multiple scenarios and also of potential problems if one is not aware of the consequences and pitfalls.

Historically speaking NAT emerged as a way to workaround the envisioned, and now real, shortage of IP addresses. This meant that if a machine did not have to be on the Internet, it also didn't need a public IP address. Therefore 3 ranges of IP addresses were created to be privately managed by private network administrators.

NAT originally appeared as a way of allowing a single, or a few, public IP address to be shared by a potentially large number of machines when accessing the Internet – this was called MASQUERADING. These machines were otherwise unreachable from the Internet, so a by-product of this measure is now seen as a security feature.

When applied blindly NAT often brings problems because many upper layer protocols encode network information on the TCP/UDP payload, or operate under the assumption that this information is not changed en-route. NAT breaks both of these principles for a lot of well-known (and also less known) protocols, like FTP, SIP, etc.

NAT is forbidden for some network level security related protocols (because the NAT **changes** packets at network level).

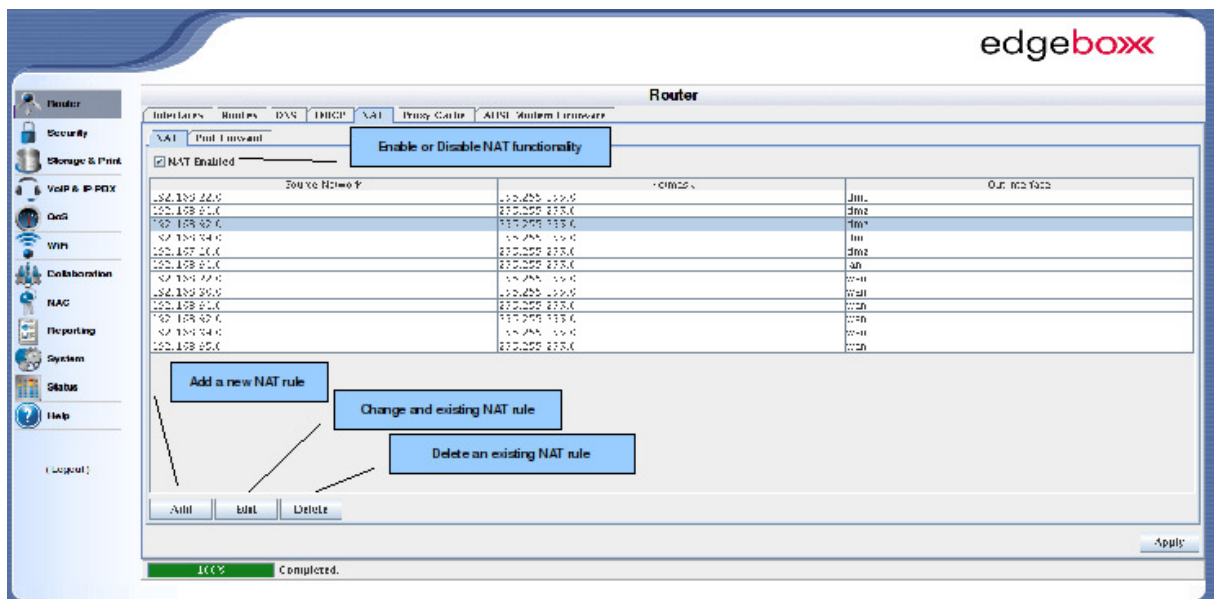
When NAT is well understood its use brings power to its users allowing for implementation of diverse scenarios that we will focus on next sections.

## NAT

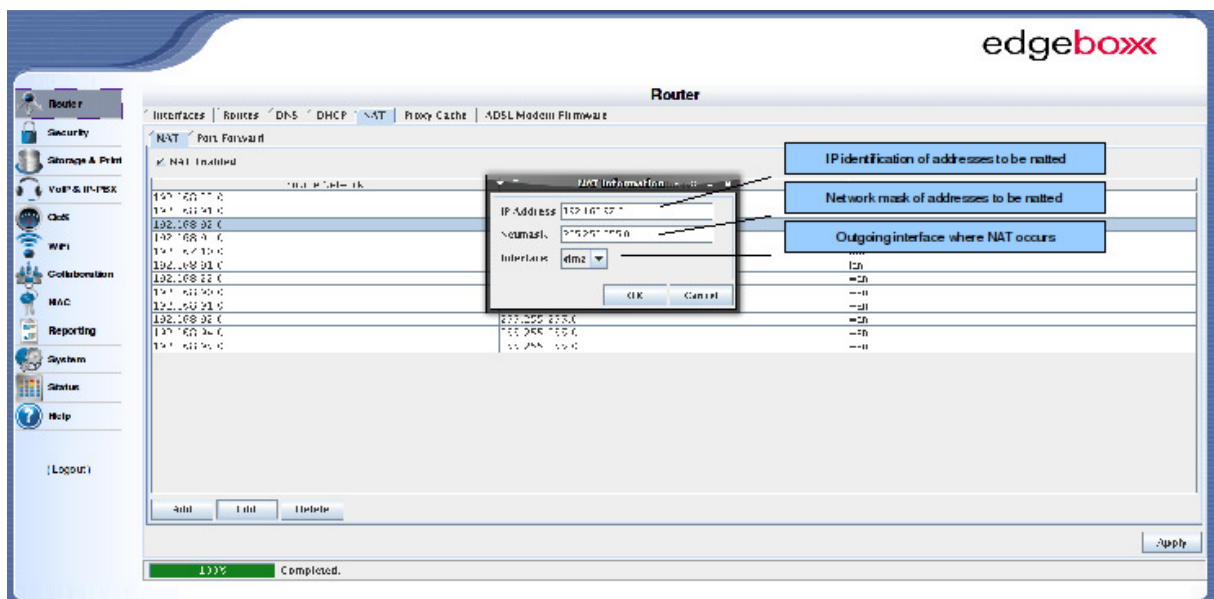
In order to have NAT functionality available, the administrator has to ensure that the NAT enabled check box is marked. After that the rules defined will become active and/or other rules can be specified.

As shown bellow, there are 3 fields relevant for defining a NAT rule:

- The IP address and Network mask together allow the identification of a variable size range of contiguous IP addresses.
- The Interface will determine where the NAT operation applies, that is to say, an admin will insert one of its LAN subnets and the WAN interface whenever he wants the users of that subnet to have full Internet access.



Main NAT panel explained

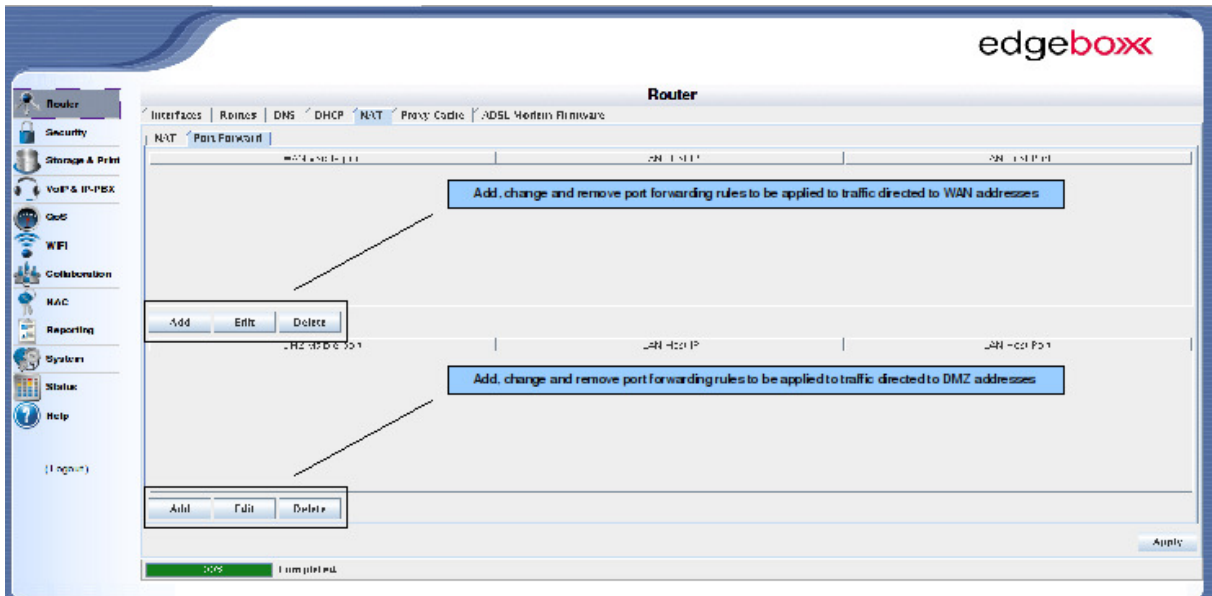


NAT rule window explained

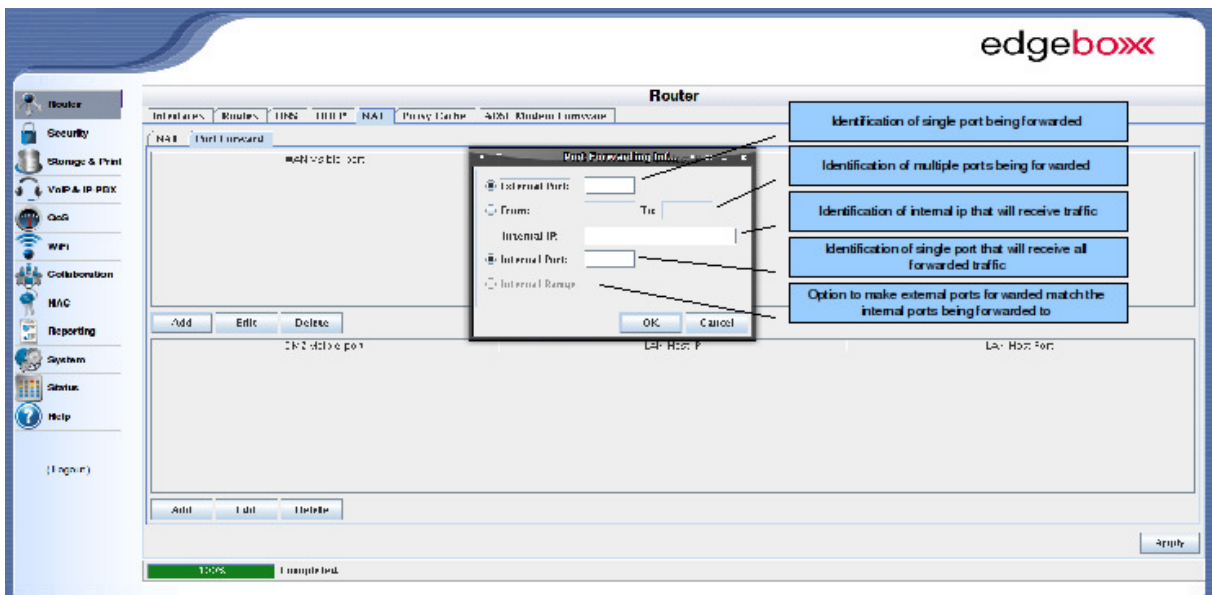
## Port forwarding (NAPT)

edgeBOX will also allow the admin to expose services running on internal LAN boxes. To expose these services public IPs on the WAN and on the DMZ interface can be used.

The next pictures are intended to explain this.



Main port forward panel explained




Port forward rule explained

There are two separate areas in the Port Forward tab to define these rules. The first one will allow the visibility of a service in an internal LAN machine using the WAN IP interface. The second one will allow the same thing but using the DMZ public IP address.

When exposing a service, the administrator can

- Forward a single public port to a single internal port
- Forward a range of public ports to a single internal port
- Forward a range of public ports to a range of internal ports

 Forwarding a port, or ports, will automatically reconfigure the firewall