

## HOWTO: Configure SNAT

### 'How-to' guides for configuring SNAT with GateDefender Integra

Panda Software wants to ensure you get the most out of GateDefender Integra. For this reason, we offer you all the information you need about the characteristics and configuration of the product. Refer to [www.pandasoftware.com/product](http://www.pandasoftware.com/product) and [www.pandasoftware.com/support](http://www.pandasoftware.com/support) for more information.

The software described in this document is delivered under the terms and conditions of the end user license agreement and can only be used after accepting the terms and conditions of said agreement.

#### Copyright notice

© Panda Software 2006. All rights reserved. Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Software, c/ Buenos Aires, 12 48001 Bilbao (Biscay) Spain.

#### Registered trademarks

Panda Software is a trademark or registered trademark belonging to Panda Software. Windows is a trademark or registered trademark of the Microsoft Corporation. Other product names that are mentioned in this guide may be registered trademarks of their respective owners.

## INDEX

1	INTRODUCTION .....	2
2	PROCEDURE .....	5
3	MOST COMMON PROBLEMS .....	8

### Symbols and styles used in this documentation

#### Symbols used in this documentation:



**Note.** Clarification and additional information.



**Important.** Highlights the importance of a concept.



**Tip.** Ideas to help you get the most from your program.



**Reference.** Other references with more information of interest.

#### Fonts and styles used in the documentation:

**Bold:** Names of menus, options, buttons, windows or dialog boxes.

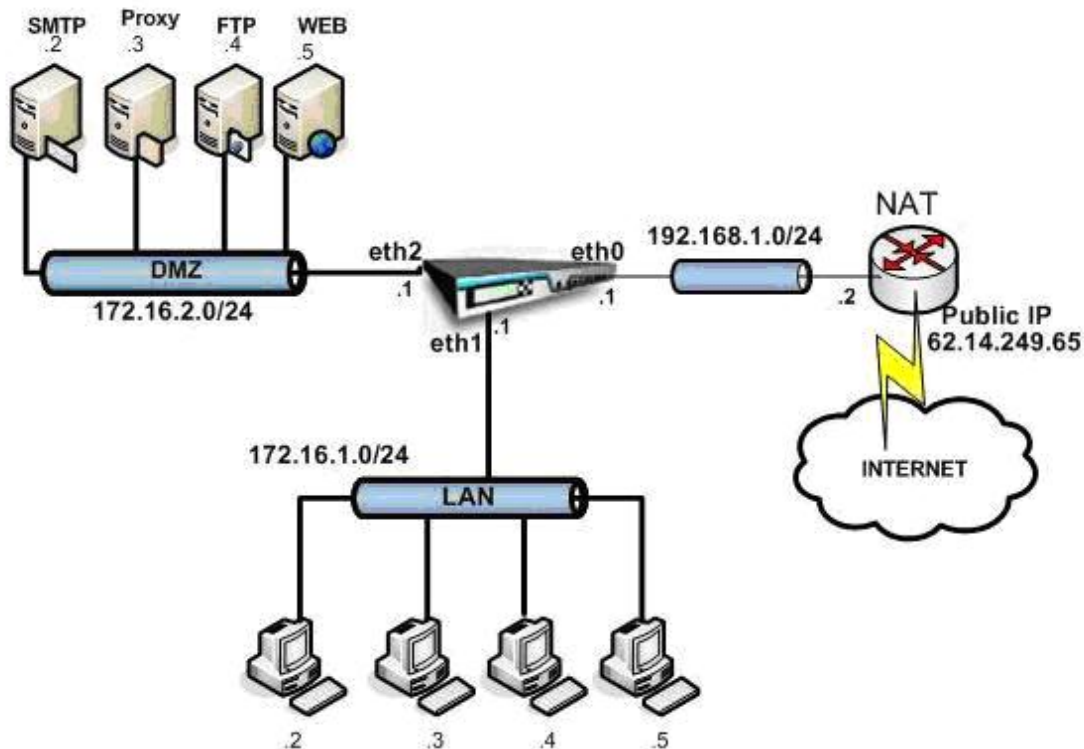
*Codes style:* Names of files, extensions, folders, command line information or configuration files, for example, scripts.

*Italics:* Names of options related with the operating system and programs or files with their own name.

# 1 Introduction

Below is an outline of the necessary steps to be taken in order to configure SNAT correctly when using Panda GateDefender Integra.

Throughout this explanation, the following network will be used as a reference point:



In this simulated set-up, Panda GateDefender Integra has been installed on the perimeter of the network in order to carry out corporate firewall functions (any other module could also be enabled along with the Firewall module).

Within this context, Integra has been configured with 3 interfaces: Eth0 for the WAN zone, Eth1 for the LAN, and Eth2 for the DMZ.

Corporate servers have been located in the DMZ.

***Normally, in the most common real set-ups, the WAN interface is given a private IP address, with an additional device providing it with WAN services - for example, an ADSL router, a cable modem, etc. - which has a public IP address (either dynamic or static). This device normally translates the Integra WAN private address to an Internet valid public address, through NAT.***

As you can see in the diagram, Integra is located behind an ADSL router which is performing the NAT for packets received through the LAN interface:

In the event that Panda GateDefender Integra is only used to route traffic (Router mode), without any extra configuration, then all traffic allowed to pass through the firewall coming

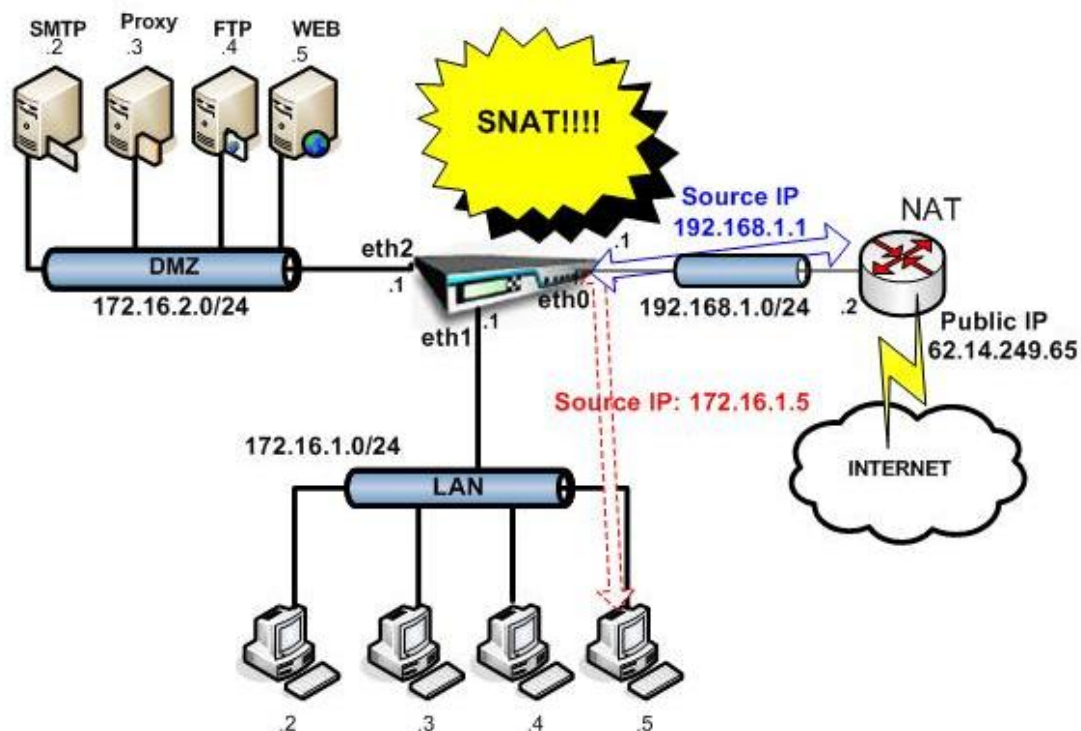
from either the LAN or the DMZ to the WAN zone will use as IP address a private IP address that belongs to these "internal" networks.

There are several methods for these packets to be routed correctly towards the Internet by the ADSL router:

- a) The ADSL router has to have in the routing table a route to reach the networks beyond Integra. To do this you can add additional static routes in the ADSL device that indicate that in order to reach these networks the external Integra interface (eth0 in this case) must be used as a Gateway.
- b) A second option that avoids any additional configuration in the ADSL device involves adding SNAT (Source NAT) rules in for internal traffic (LAN and DMZ) towards the WAN. In this way, the ADSL router will receive all the packets with an IP address belonging to the network 192.168.1.0/24 which it can access through the LAN interface.

The ADSL device will then apply NAT once again on these Internet-bound packets using the public IP address assigned in the WAN interface.

Below you will see a graph showing a SNAT rule in Panda GateDefender Integra:



The rule to be entered will make the LAN host 172.16.1.5 appear in the WAN zone between Integra and the ADSL router, and with the address 192.168.1.1. in its packets' headers.

[Index](#)

## 2 Procedure

The first factor to bear in mind is that NAT (SNAT/DNAT) is not enabled by default when Integra is working in Router mode. In this working mode, Integra's only role is to route the traffic.

In order to enable SNAT, the firewall needs to be configured with SNAT rules, which differ from normal filtering rules.

In the same way as filtering rules are established, a pre-configuration of IP addresses and networks can be carried out through the *IP addresses* section in the *Definitions* menu in order to simplify rule management.

Follow the steps below according to the defined scenario:

1. Network definitions are entered which might be useful when configuring rules.

The screenshot displays two configuration panels. The top panel, titled 'Addresses', contains a table with the following data:

Name	Addresses
ip_Eth0	192.168.1.1

Below the table are buttons for 'Export', 'Import', 'Add', 'Modify', and 'Delete'. The bottom panel, titled 'Groups', contains a table with the following data:

Name	Addresses
LAN	172.16.1.0/ 24
DMZ	172.16.2.0/ 24

Below this table are also buttons for 'Export', 'Import', 'Add', 'Modify', and 'Delete'.

In this case, the range of LAN and DMZ networks are defined as well as the IP address assigned to the WAN interface.



**Note:** This step is not obligatory - addresses can be entered without having defined ranges first, although in the event that there are a large number of rules to be entered, pre-defining them significantly simplifies the task.

2. A new rule is added:

Select SNAT as the action to be taken:

3. The rest of the parameters can now be configured:

- A name is assigned to the rule.
- The source and target properties of the packets which are subjected to the NAT process are selected. This selection can be made in a number of ways: via interface, zone or IP address. In this case, the user wishes to subject all traffic from LAN (interface eth1) heading for the Internet (interface eth0) to the NAT process.
- The services to which SNAT rules are to be applicable are selected. In this case, they are to be applied to all types of traffic.

The following parameters indicate Panda GateDefender Integra which IP address or addresses have to be used for translation purposes: In this case, there is only one IP address in the WAN interface, which has been defined as a IP address Eth0, and will be used to NAT all requests that come from any LAN device.

If the *Keep source address* option is selected, a SNAT rule will be applied, although the packet's source IP will not be modified. This may be useful in certain specific situations, such as when configuring a VPN IPSEC in a NAT environment.

The *Address group* field is used in the event that there are a number of addresses for changing the source header, and not just one.

From here, the priority which is to be assigned to the new rule can be entered, thus establishing the priority of the rule within the context of all SNAT rules. If this field is not altered, the rule will be placed after the last established SNAT rule.

Finally, there will only be optional parameters left, which can be configured in order to establish the rule so that it is applied at certain times, or the option that allows all packets to be subjected to the specific characteristics of the SNAT rule to be logged.

Schedule:  Schedule settings

Create log

Comment (max. 255 characters)

Once the rule has been added, it can then be seen in the list of SNAT rules

**Filtering rules**

DNAT Filter **SNAT**

Active	Name	Source	Target	Service	Action	Schedule
<input checked="" type="checkbox"/>	SNAT Internet	LAN	WAN	All	SNAT	None

1/1/2014 10:22:24

[Index](#)

### 3 Most Common Problems

One of the most common problems that arise when configuring SNAT is the blocking of SNAT traffic due to the firewall's own filtering rules. In addition to establishing SNAT rules, it will therefore also be necessary to ensure that the firewall rules allow this type of traffic to pass unhindered.

Filtering rules

Active	Name	Source	Target	Schedule	Service	Action
<input checked="" type="checkbox"/>	PING	All	All	None	PING	Allow
<input checked="" type="checkbox"/>	TELNETegress	All	WAN	None	Telnet	Allow
<input checked="" type="checkbox"/>	FTPEgress	All	WAN	None	FTP	Deny
<input checked="" type="checkbox"/>	HTTPegress	All	WAN	None	HTTP	Allow
<input checked="" type="checkbox"/>	HTTPSegress	All	WAN	None	HTTPS	Allow
<input checked="" type="checkbox"/>	SMTPegress	All	WAN	None	SMTP	Allow
<input checked="" type="checkbox"/>	DNSegress	All	WAN	None	DNS	Allow
<input checked="" type="checkbox"/>	POP3egress	All	WAN	None	POP3	Allow
<input checked="" type="checkbox"/>	IMAPEgress	All	WAN	None	IMAP	Allow
<input checked="" type="checkbox"/>	EgressProh...	All	WAN	None	All	Deny
<input checked="" type="checkbox"/>	DENY	All	All	None	All	Deny

In this example, those systems which are to make use of SNAT services from the LAN will be able to access Internet without any problems by using HTTP browsers. However, in spite of the established SNAT rule, FTP traffic to the Internet will not be permitted, as there is a filtering rule which prevents it.

A specific configuration which should be avoided, as it can create problems with traffic that has been NATted incorrectly, is that of selecting the **Any** option in both the source and target fields when creating a SNAT rule.

[Index](#)