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 and www.pandasoftware.com/support for more information.

‘How-to’ guides for Panda GateDefender Integra

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

Registered trademarks

D.L. BI-3269-05

INDEX

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.

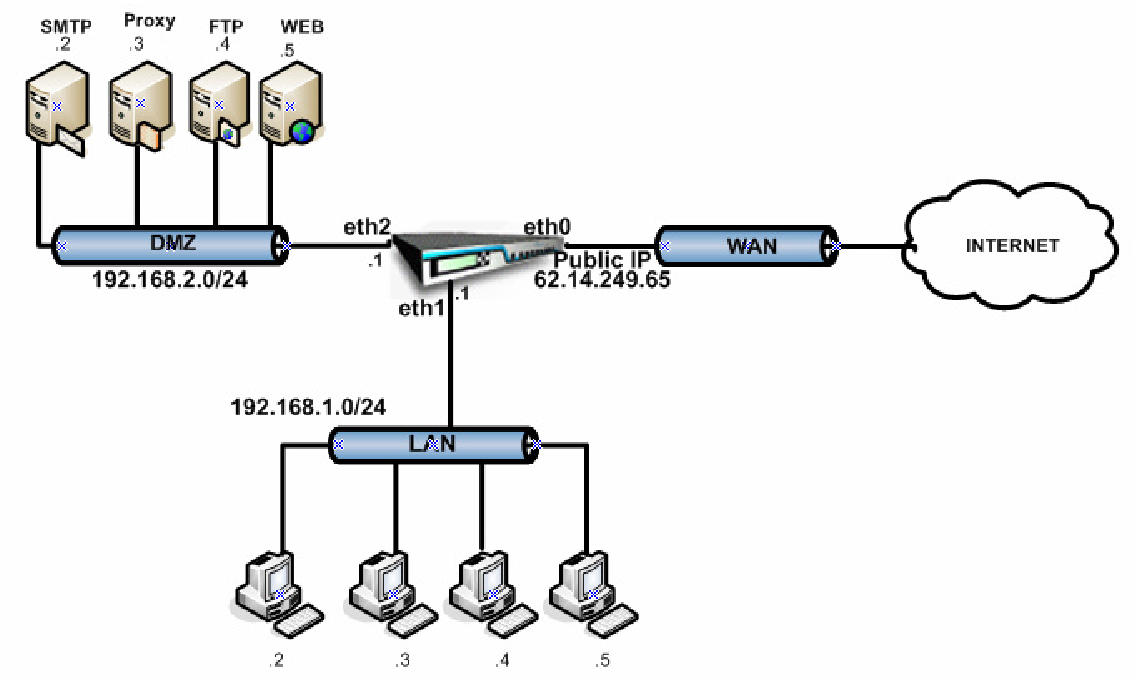
Fonts and styles used in the documentation:

Bold	Names of menus, options, buttons, windows or dialog boxes.
`Code 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.

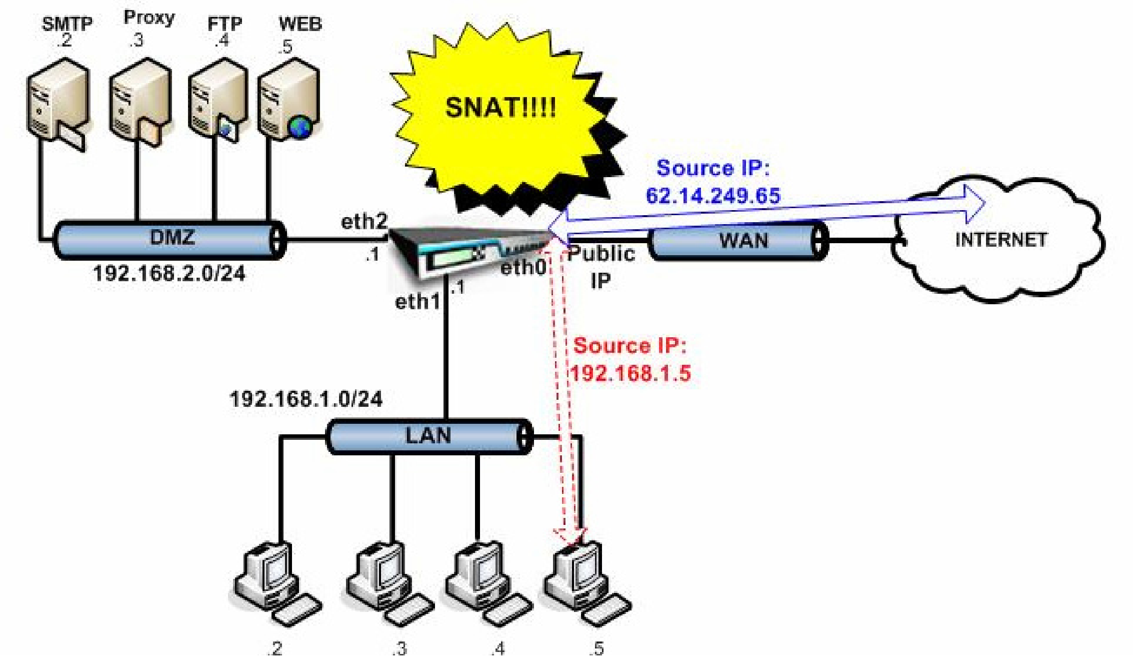
The diagram shows how the Eth0 interface has been given a public IP address. Normally, in the most common real set-ups, the WAN interface is given a private IP address, with an additional device providing it with WAN services - for example, an ADSL router, a cable modem, etc. - which has a public IP address (either dynamic or static). This device normally translates the Integra WAN private address to an Internet valid public address, through NAT.

We have used this version in order to simplify the procedure and make it more intuitive.

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 (if this is enabled) coming from either the LAN or the DMZ to the WAN zone will be assigned a private IP address for these areas in the source IP field, meaning that it will not reach the Internet as it does not have a valid public IP address.

So that all the devices located in the company's internal network (LAN or DMZ) can reach the Internet, the SNAT function featured in the Firewall module can be employed.

Below is an explanation of how to set up a SNAT rule that allows Internet access to LAN users by using the public IP address assigned to the WAN interface:



With the rule to be entered, the LAN host 192.168.1.5 will reach the Internet with the 62.14.249.65 address in the packet headers, an IP address assigned to the WAN interface and valid for Internet purposes.

2 Procedure

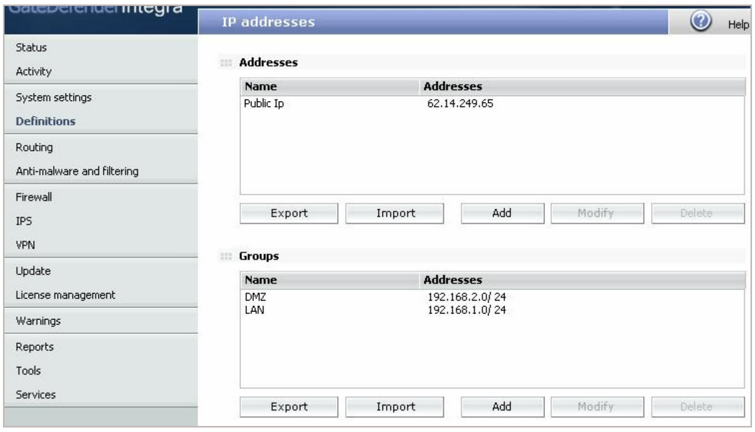
The first factor to bear in mind is that NAT (SNAT/DNAT) is not enabled by default when Integra is working in Router mode. In this working mode, Integra’s only role is to route the traffic.

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.



Addresses

Name	Addresses
Public Ip	62.14.249.65

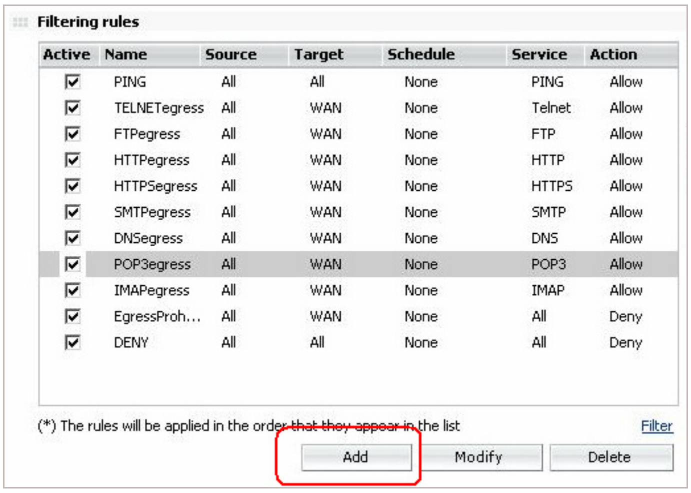
Groups

Name	Addresses
DMZ	192.168.2.0/ 24
LAN	192.168.1.0/ 24

In this case, the range of LAN and DMZ networks are defined as well as the public 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:

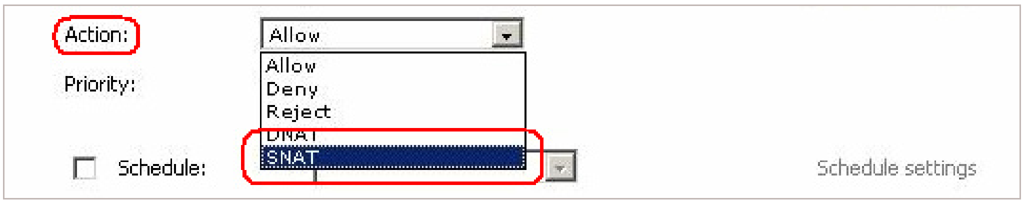


Filtering rules

Active	Name	Source	Target	Schedule	Service	Action
☑	PING	All	All	None	PING	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Allow
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	WAN	None	HTTPS	Allow
☑	SMTPegress	All	WAN	None	SMTP	Allow
☑	DNSegress	All	WAN	None	DNS	Allow
☑	POP3egress	All	WAN	None	POP3	Allow
☑	IMAPegress	All	WAN	None	IMAP	Allow
☑	EgressProh...	All	WAN	None	All	Deny
☑	DENY	All	All	None	All	Deny

(*) The rules will be applied in the order that they appear in the list

Select SNAT as the action to be taken:

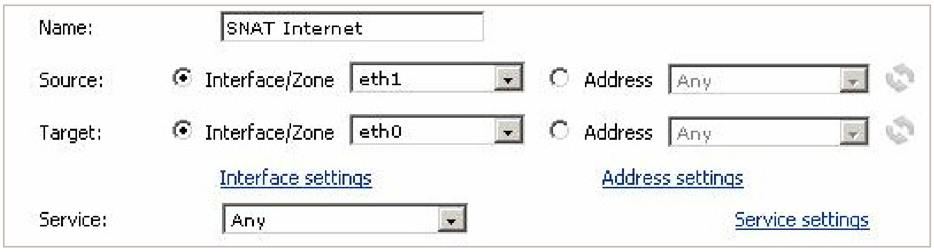


Action: Allow

Priority:

□ Schedule:

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



Name: SNAT Internet

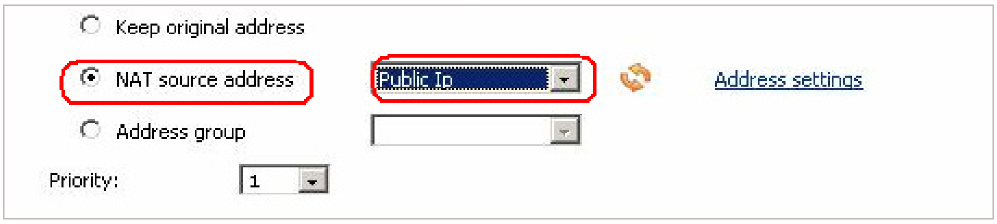
Source: ● Interface/Zone eth1 ○ Address Any

Target: ● Interface/Zone eth0 ○ Address Any

Service: Any

- 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:



○ Keep original address

● NAT source address Public Ip

○ Address group

Priority: 1

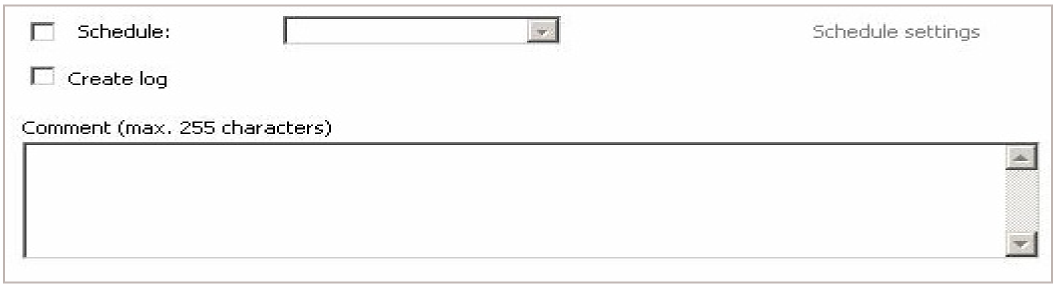
In this case, there is only one IP address in the WAN interface, which has been defined as a Public IP, and will be used to NAT all requests that come from any LAN device.

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.

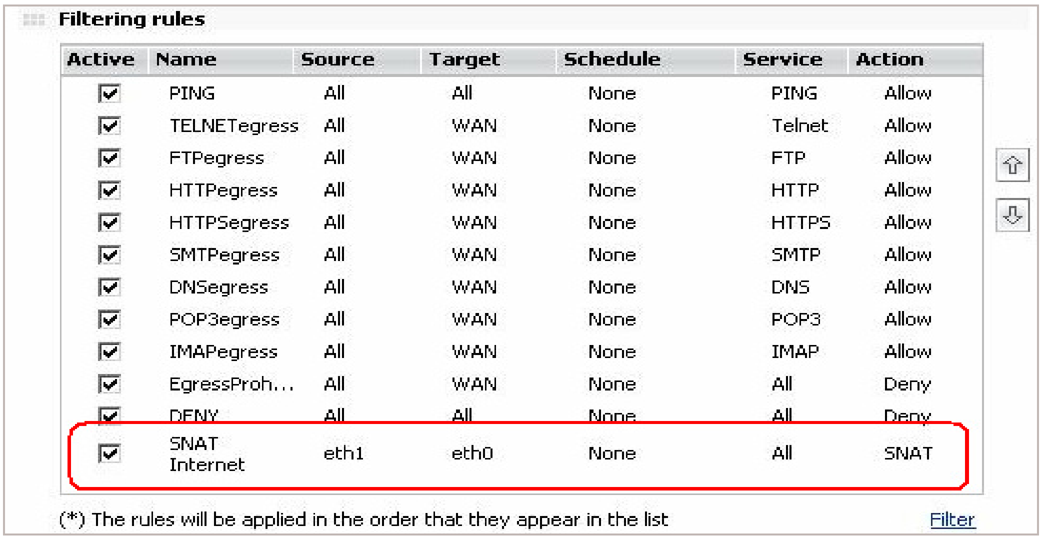


□ Schedule: Schedule settings

□ Create log

Comment (max. 255 characters)

Once the rule has been added, it can then be seen in the list of SNAT rules (appearing after the filtering rules):



Filtering rules

Active	Name	Source	Target	Schedule	Service	Action
☑	PING	All	All	None	PING	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Allow
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	WAN	None	HTTPS	Allow
☑	SMTPegress	All	WAN	None	SMTP	Allow
☑	DNSegress	All	WAN	None	DNS	Allow
☑	POP3egress	All	WAN	None	POP3	Allow
☑	IMAPegress	All	WAN	None	IMAP	Allow
☑	EgressProh...	All	WAN	None	All	Deny
☑	DENY	All	All	None	All	Deny
☑	SNAT Internet	eth1	eth0	None	All	SNAT

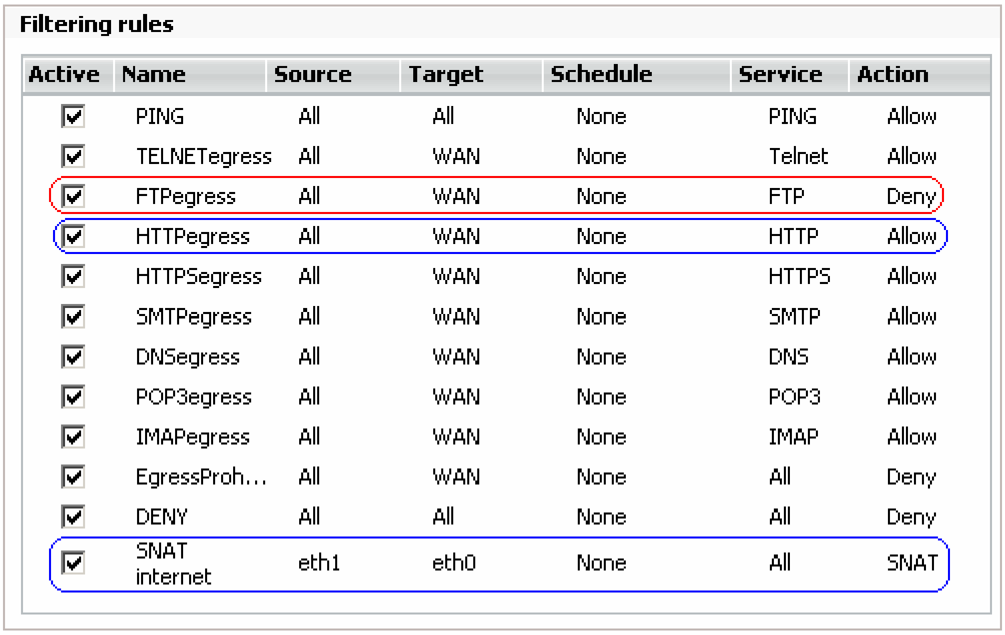
(*) The rules will be applied in the order that they appear in the list

Filter

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.

For example, the set of rules shown below features a SNAT rule which is applicable to all traffic passing from the LAN to the WAN:



Filtering rules

Active	Name	Source	Target	Schedule	Service	Action
☑	PING	All	All	None	PING	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Deny
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	WAN	None	HTTPS	Allow
☑	SMTPegress	All	WAN	None	SMTP	Allow
☑	DNSegress	All	WAN	None	DNS	Allow
☑	POP3egress	All	WAN	None	POP3	Allow
☑	IMAPegress	All	WAN	None	IMAP	Allow
☑	EgressProh...	All	WAN	None	All	Deny
☑	DENY	All	All	None	All	Deny
☑	SNAT internet	eth1	eth0	None	All	SNAT

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.