Panda GateDefender Integra

Configure DNAT in order to publish internal services via Internet

'How-to' guides for configuring DNAT 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

Copyright notice

Registered trademarks

D.L. BI-3269-05

Index

1 INTRODUCTION 3

2 PROCEDURE 5

2.1 EXAMPLE 1 5
2.2 EXAMPLE 2 9

3 MOST COMMON PROBLEMS 13

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.

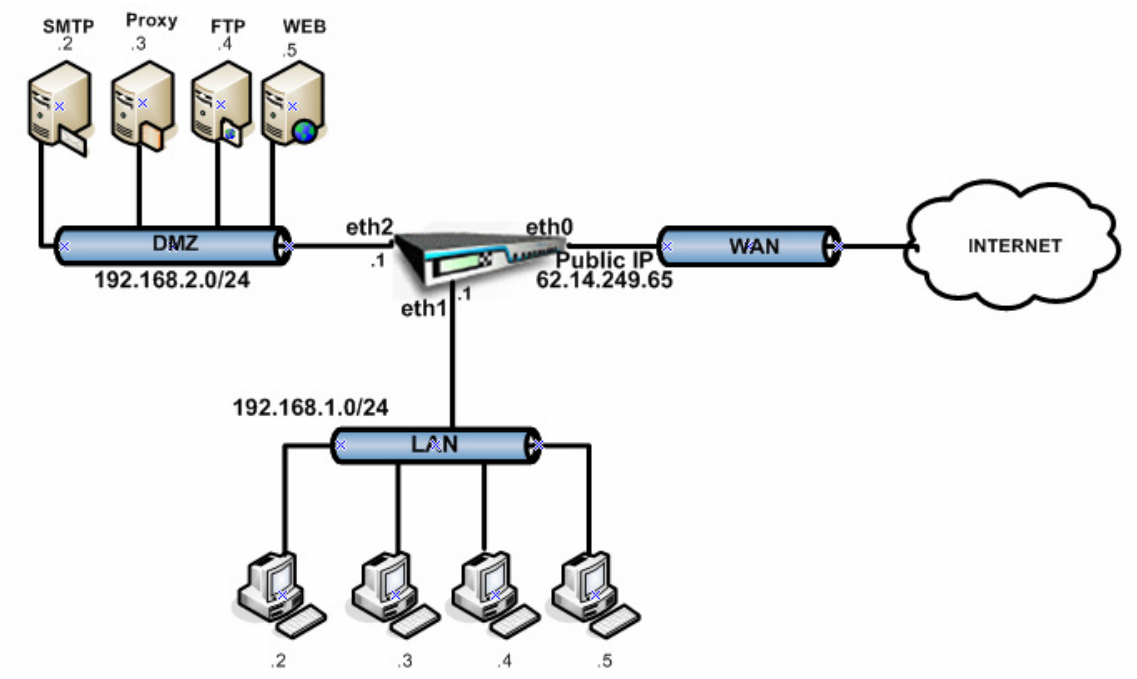
Fonts and styles used in the documentation:

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 set up DNAT correctly in Panda GateDefender Integra and to be able to publish internal services via Internet.

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.

Here it is assumed that Integra has already been configured with SNAT rules, and that both the LAN and the DMZ are therefore transparent beyond the Integra's WAN interface, the IP address of which is the only network "representative" which protects Panda GateDefender Integra.

In other words, the only way of reaching both Integra and its internal networks (LAN and DMZ in this case) is via the public IP address that has been assigned to the device.

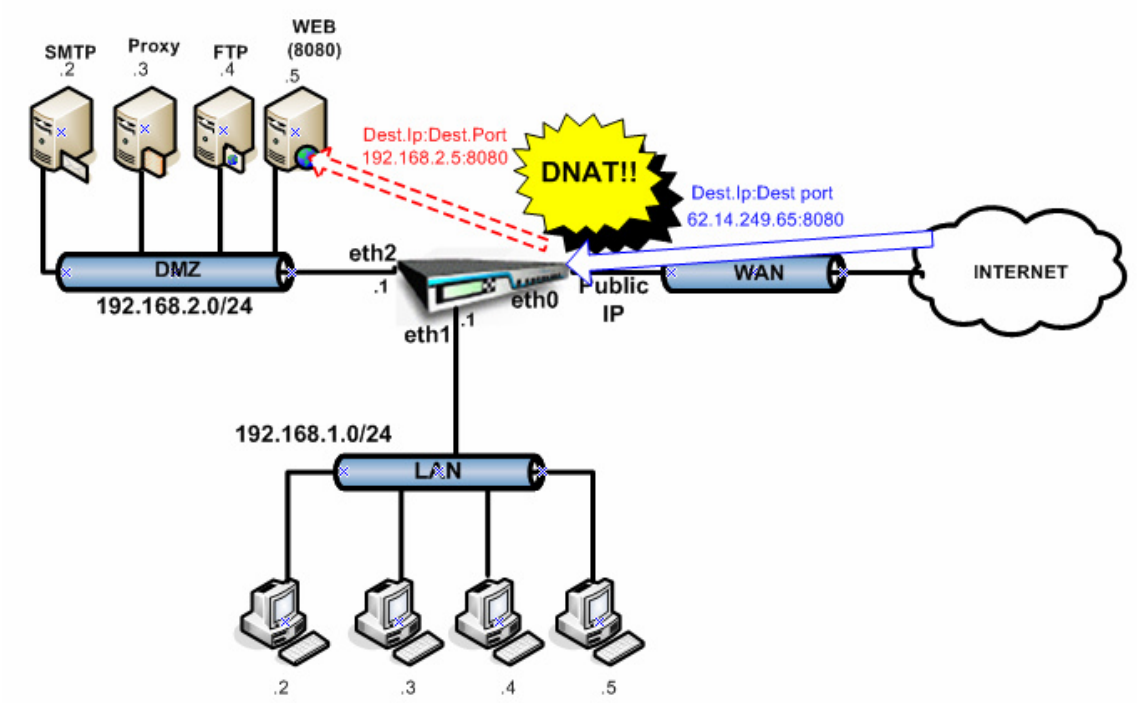
As the internal networks are "hidden", in order to be able to reach the DMZ servers in the event that the user wishes to publish their services, the user will need to set up an advanced configuration, adding DNAT rules, a technique which is also known as Port Forwarding.

What follows is a number of different scenarios, with explanations as to how the necessary configurations can be set up in order to publish the services offered by the DMZ servers.

2 Procedure

2.1 Example 1

As it can be seen in the following scenario, the DMZ web server is offering services in port 8080:



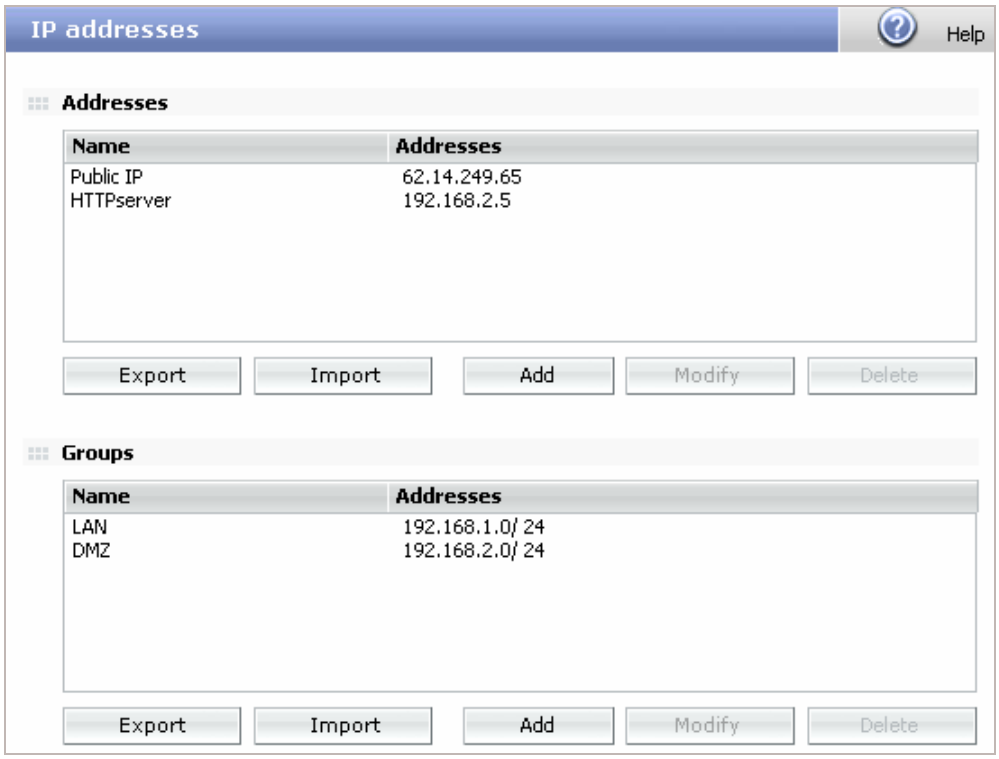
In order to be able to access this hidden service from the Internet through Integra's firewall, static mapping can be carried out in such a way as to allow the traffic that reaches Integra's WAN port via port 8080 to be redirected to the internal WEB server at the same port.

With this set up, requests to Integra's public IP address via port 8080 pass though Integra, which then replaces the target IP address with the private IP address of the DMZ web server.

In order to do this, it is necessary to add a DNAT rule to the firewall.

Follow the steps below according to the defined scenario:

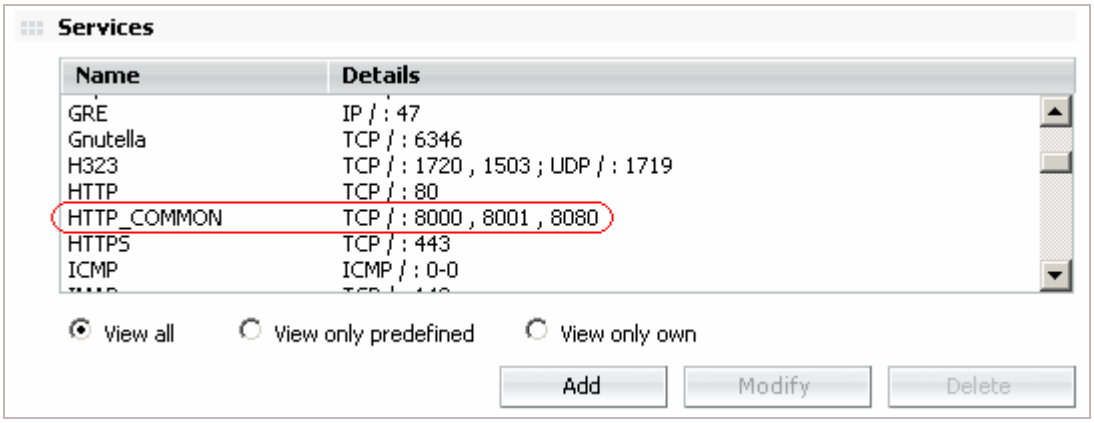
1. Network definitions are entered which might be useful when configuring rules.



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

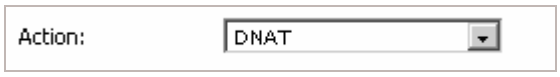
Note: This step is not obligatory - addresses can be entered without having defined ranges first, although in the event that there are a large number of rules to be entered, pre-defining them significantly simplifies the task.

2. The service which is to be mapped is first defined. In this case it is not necessary to enter a new service as there is already an HTTP service in port 8080 in the predefined default services:

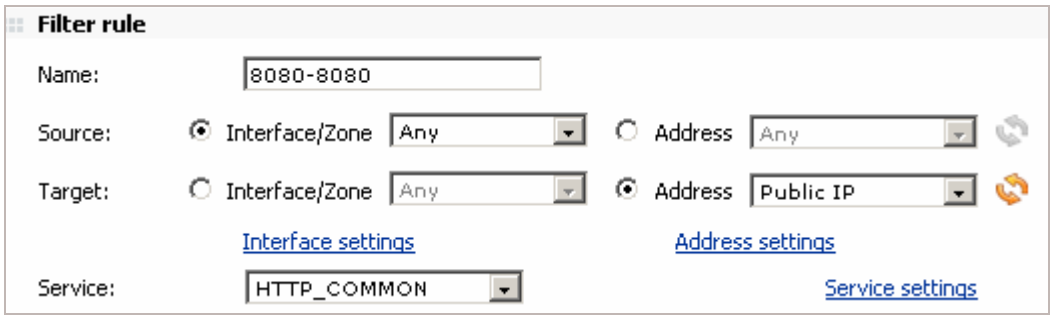


3. A DNAT rule is then added which maps HTTP traffic to the internal web server via port 8080:

   A DNAT action is then selected, thus creating a DNAT rule:

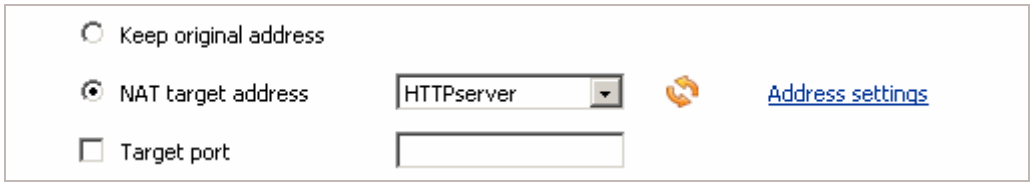


A name is assigned to the rule, and the characteristics of the traffic which will be affected by this rule are then defined:



- The rule is applied to traffic coming from any source, as the source of requests from the Internet is not known.
- The IP address of the interface receiving this traffic should be selected as the target, in this example, the web interface to which a public IP address has been assigned.
- The service to which the rule is to be applied in our example is HTTP_COMMON, predefined by default, and which includes HTTP traffic via port 8080.

4. The parameters of the final target of the static mapping are then defined:



In the **NAT target address** field, the target server for the HTTP request should be entered. In this case, we can use the definition which has been entered for the DMZ web server, instead of directly entering the IP address.

If you select **Keep source address**, the target header will not change. This option can be used in special circumstances.

The **Target Port** option in this case is not necessary as it is not going to change.

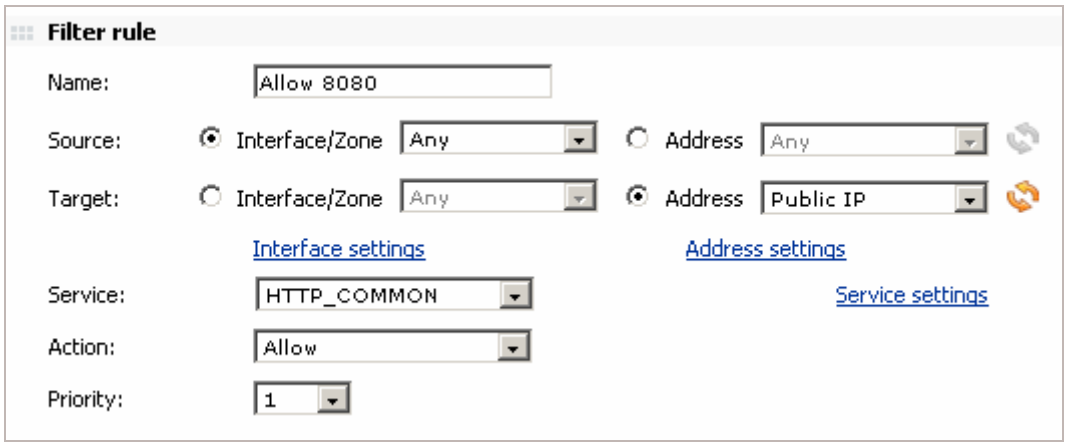
5. The other optional parameters dealing with data logging, rule schedule, etc. can now be defined.

Once all parameters have been defined, the rule will appear as shown here:

Once the DNAT rule has been entered, it is necessary to ensure that the traffic to be redirected is not blocked by the firewall's filter rules.

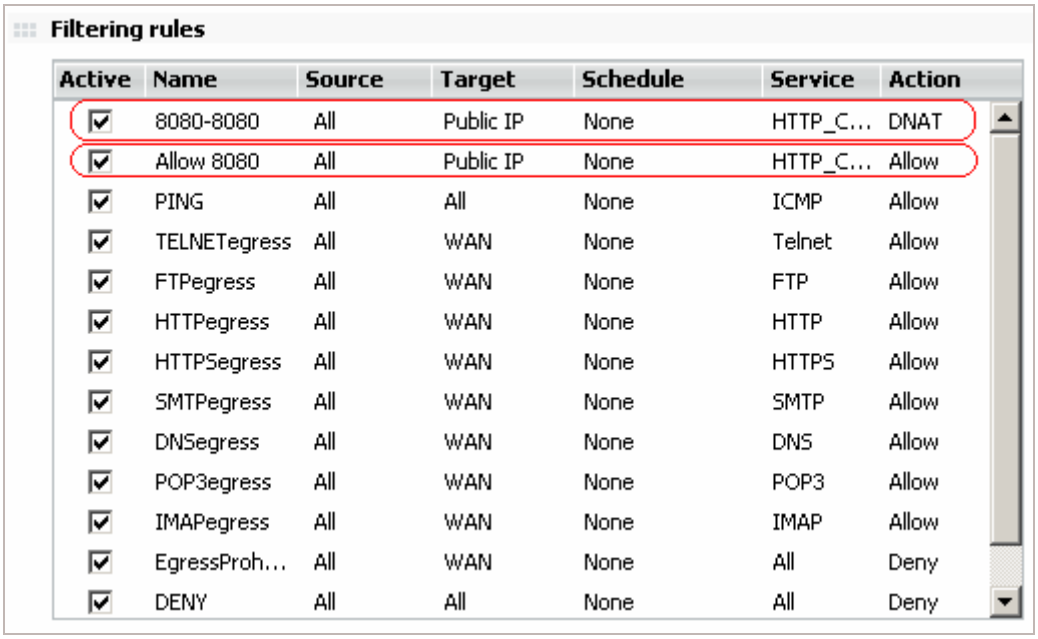
In this case, the default rules block HTTP traffic via port 8080, making it necessary to enter a rule which will allow such traffic:

In order to do this, a new filter rule must be set up as shown here:



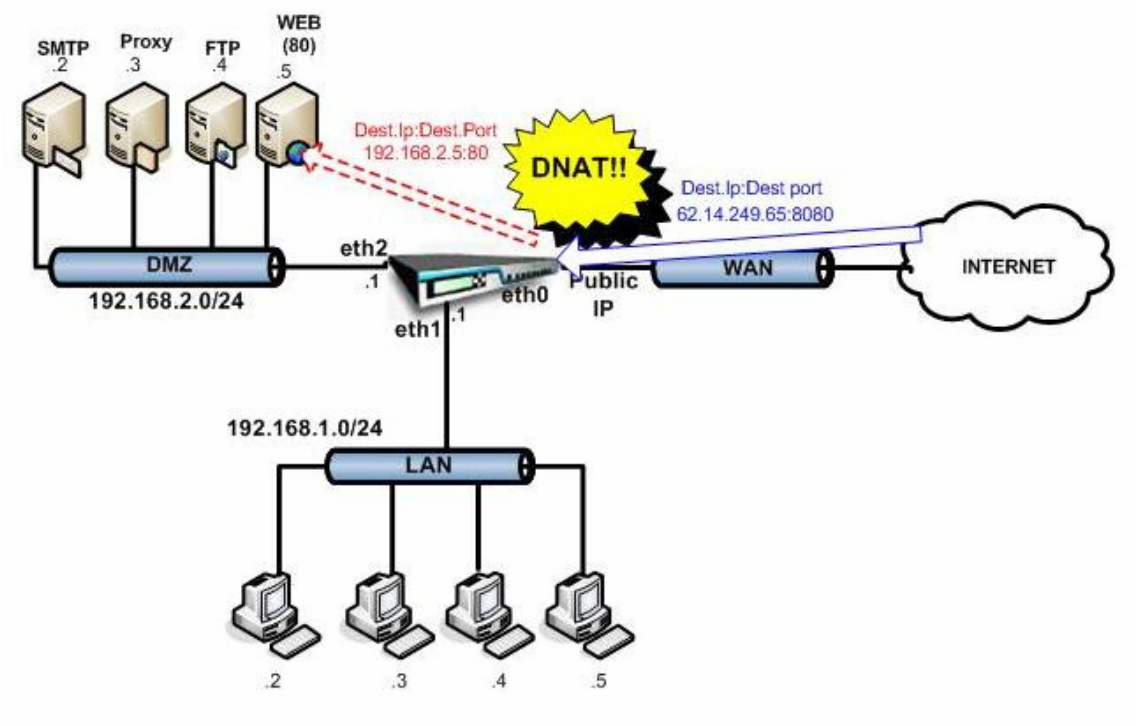
This rule allows incoming traffic from any source to pass to the public IP address assigned to the web interface and whose target ports are included in the service defined as HTTP_common, including port 8080.

These filter rules, along with the defined DNAT rule, will redirect traffic that reaches Integra via the WAN interface to port 8080 on the DMZ web server.



2.2 Example 2

In this example, you should proceed as in Example 1, with the only difference being that in this case, the web server offers its services via port 80, although publicly it continues to offer them via 8080. In this case, in addition to changing the target IP address, the target port will also have to be changed from 8080 to 80.



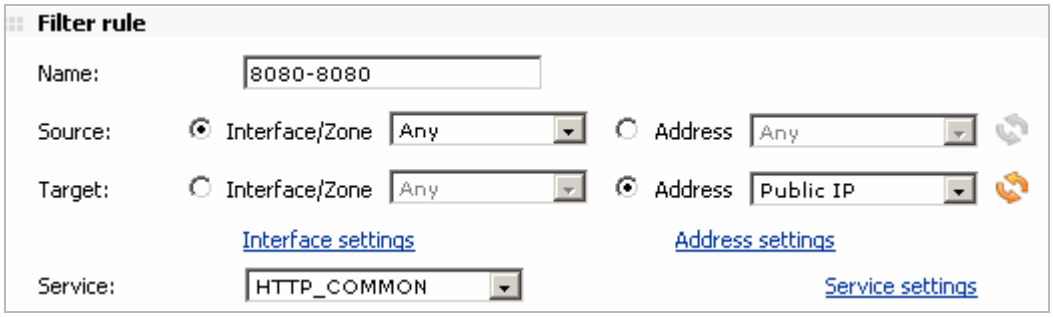
In order to do this, it is necessary to add a DNAT rule to the firewall.

Follow the steps below according to the defined scenario:

1. The same network and service definitions as in Example 1 are entered.
2. A DNAT rule is then added which maps HTTP traffic to the internal web server via port 8080::

   A DNAT action is then selected, thus creating a DNAT rule:

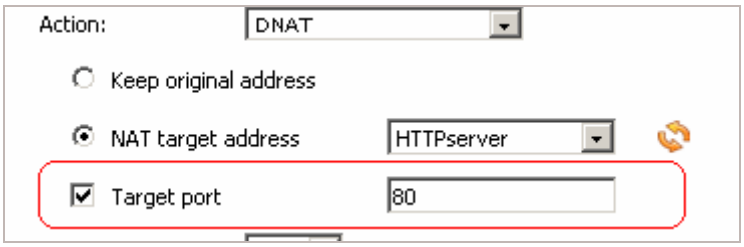
   A name is given to the rule, and the characteristics of the traffic which will be affected by this rule are then defined:



   - The rule is applied to traffic coming from any source, as the source of requests from the Internet is not known.
   - The IP address of the interface receiving this traffic should be selected as the target- in this example, the web interface to which a public IP address has been assigned.

- The service to which the rule is to be applied in our example is HTTP_COMMON, predefined by default, and which includes HTTP traffic via port 8080.

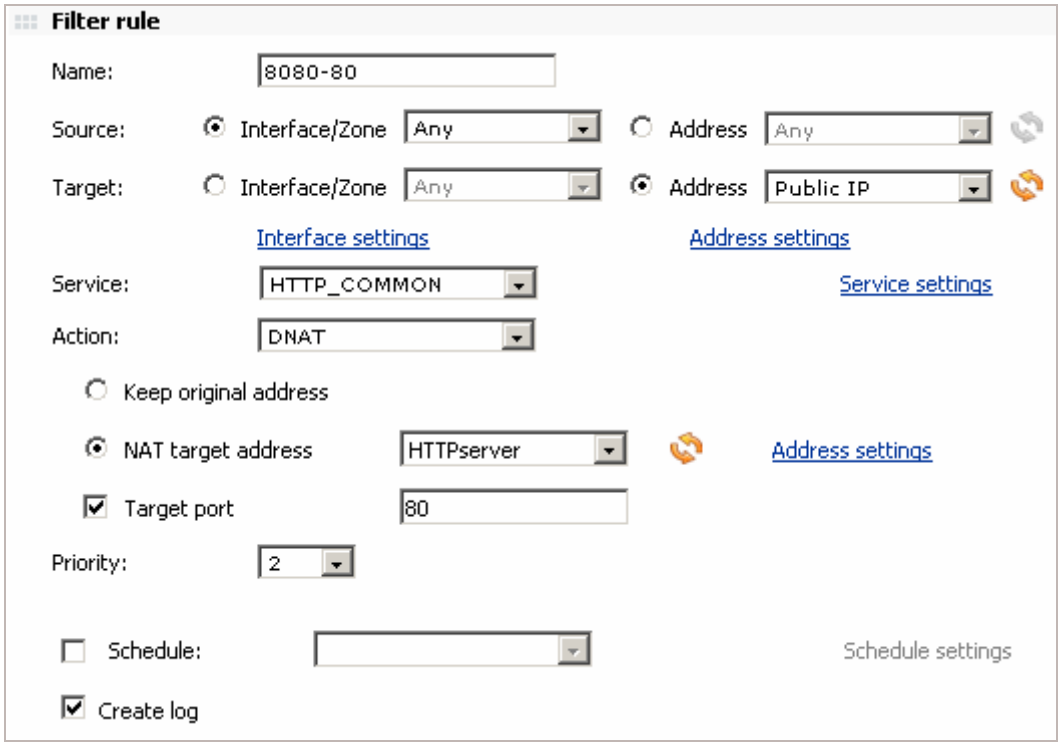
3. The parameters of the final target of the static mapping are then defined:



In this example, as the target port needs to be changed, you have to check the corresponding checkbox and enter the real target port that the server is listening on, in this case, port 80.

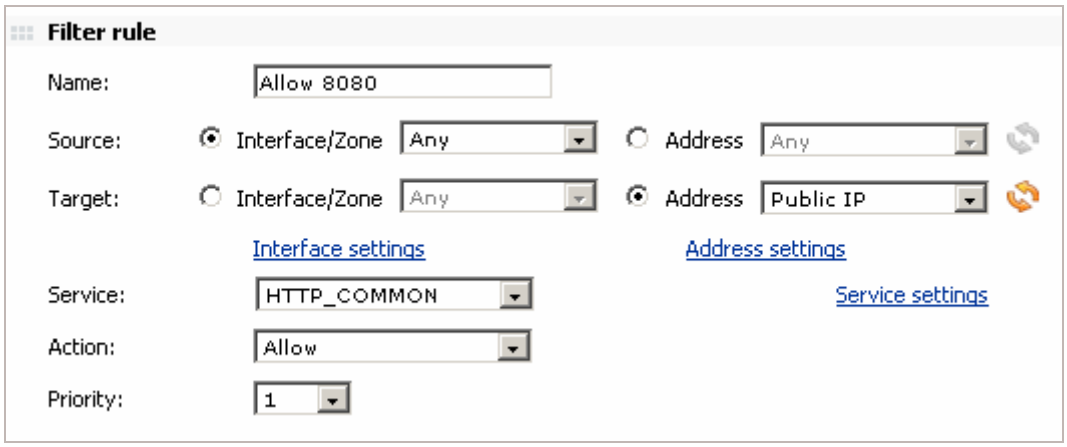
4. The other optional parameters dealing with data logging, rule schedule, etc. can now be defined.

Once all parameters have been defined, the rule will appear as shown here:



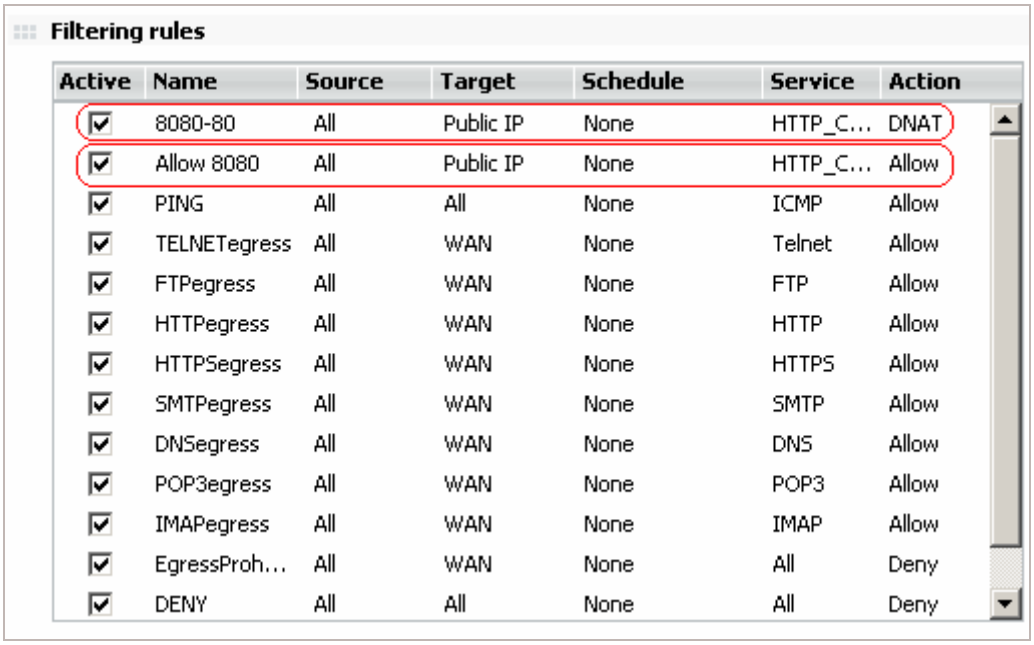
As in the previous example, filter rules should not block the incoming traffic which needs to be redirected.

In order to do this, a new filter rule must be set up, as shown here:



This rule allows incoming traffic from any source to pass to the public IP address assigned to the web interface and whose target ports are included in the service defined as HTTP_common, including port 8080.

These filtering rules, along with the defined DNAT rule, will redirect traffic that reaches Integra through port 8080 via the WAN interface to port 80 on the DMZ web server.

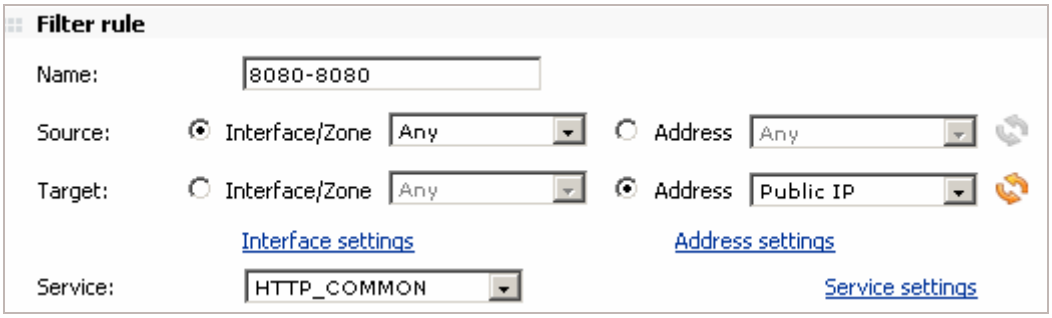


Active	Name	Source	Target	Schedule	Service	Action
☑	8080-80	All	Public IP	None	HTTP_C...	DNAT
☑	Allow 8080	All	Public IP	None	HTTP_C...	Allow
☑	PING	All	All	None	ICMP	Allow
☑	TELNETegress	All	WAN	None	Telnet	Allow
☑	FTPegress	All	WAN	None	FTP	Allow
☑	HTTPegress	All	WAN	None	HTTP	Allow
☑	HTTPSegress	All	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

3 Most Common Problems

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

Another typical problem you might encounter is the incorrect definition of the parameters which define the traffic to which the DNAT rule is to be applied. In this case, you need to ensure that the target IP field refers to the interface to which incoming traffic is to be redirected. In the previous examples, this would be the Integra public IP address refering to the eth0 interface.



0906-PGDIHT03-01-EN