configure access to the Web console in two Integra interfaces when using DNAT

'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

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:

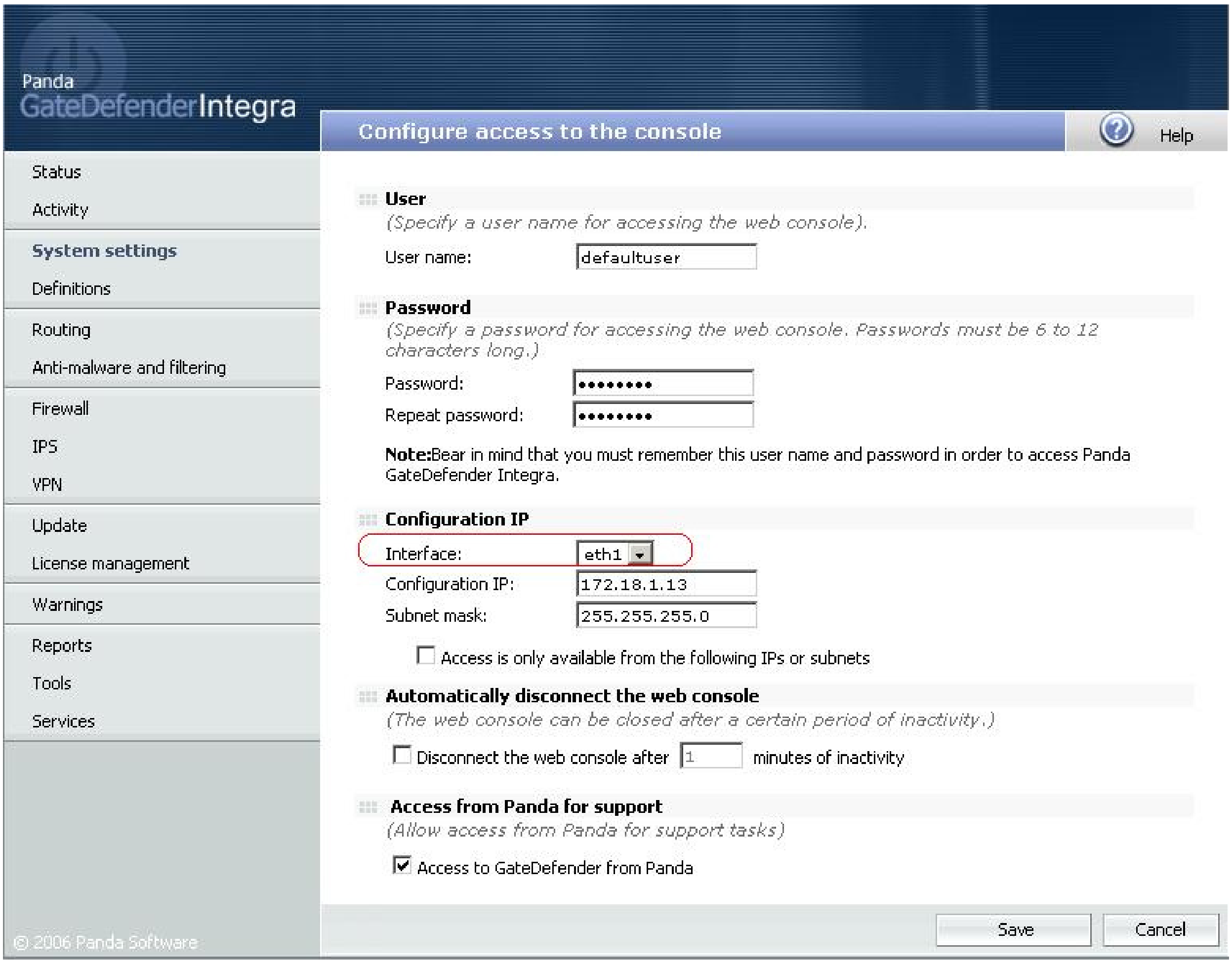
Note. Clarification and additional information.
Important. Highlights the importance of a concept.
Tip. Ideas to help you get the most from your program.
Reference. Other references with more information of interest.

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

Panda GateDefender Integra lets you access the Web console from a single interface. This access from a single interface can be configured from the **Console access** sub-menu in the **System settings** menu:



Configure access to the console

User
(Specify a user name for accessing the web console).
User name: defaultuser

Password
(Specify a password for accessing the web console. Passwords must be 6 to 12 characters long.)
Password: ••••••••
Repeat password: ••••••••

Note: Bear in mind that you must remember this user name and password in order to access Panda GateDefender Integra.

Configuration IP
Interface: eth1
Configuration IP: 172.18.1.13
Subnet mask: 255.255.255.0
□ Access is only available from the following IPs or subnets

Automatically disconnect the web console
(The web console can be closed after a certain period of inactivity.)
□ Disconnect the web console after 1 minutes of inactivity

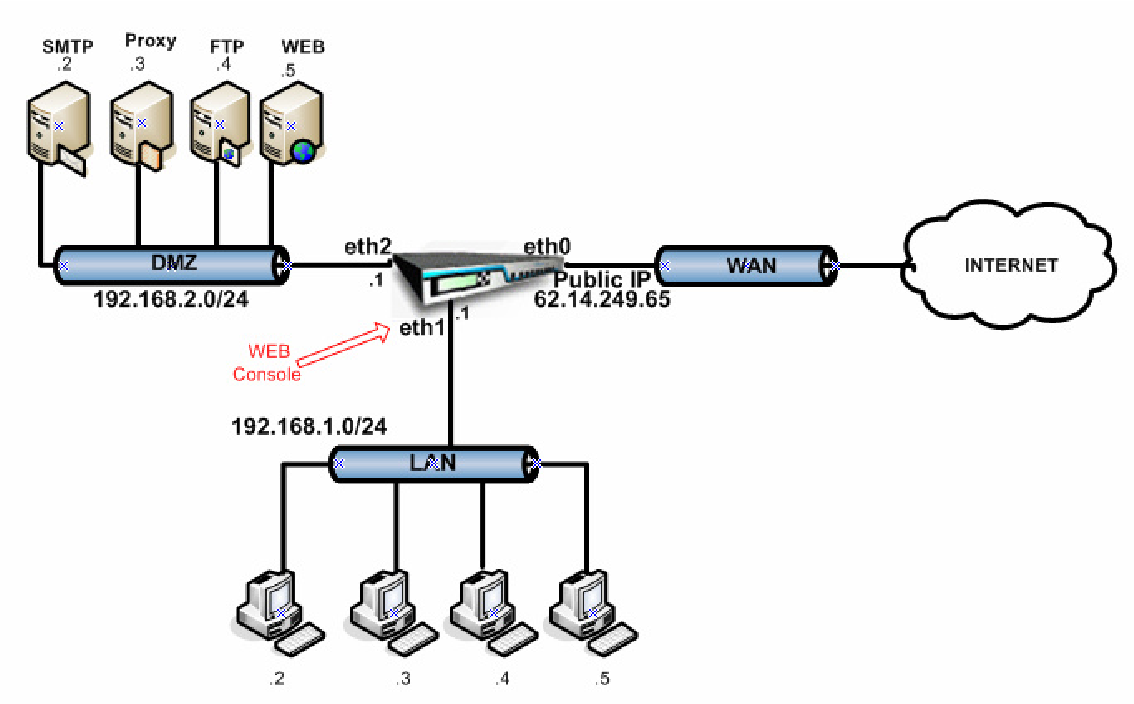
Access from Panda for support
(Allow access from Panda for support tasks)
☑ Access to GateDefender from Panda

Save Cancel

Normally, access to the Web console is configured in one of the internal network interfaces (LAN or DMZ), as this is more secure than the WAN interface.

However, it can be useful on occasions for Web console access to be enabled on several interfaces. For example, if Panda Software's tech support department requests remote HTTPS access to the machine to resolve an incident, it is not necessary to change the console settings. Using a simple DNAT rule it is possible to allow access to the Web console both on the LAN and WAN ports.

To illustrate how to do this, we will use the following network as an example:



In this simulation a Panda GateDefender Integra unit has been placed in the network perimeter to carry out corporate firewall functions (any other module can also be enabled along with the Firewall).

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

NOTE: This example is used in order to simplify the how-to and make it more intuitive.

We are obviously taking for granted that Integra has been configured with SNAT rules, so both the LAN and the DMZ are transparent beyond the Integra WAN interface, whose IP is the sole "representative" of the network protected by Panda GateDefender Integra.

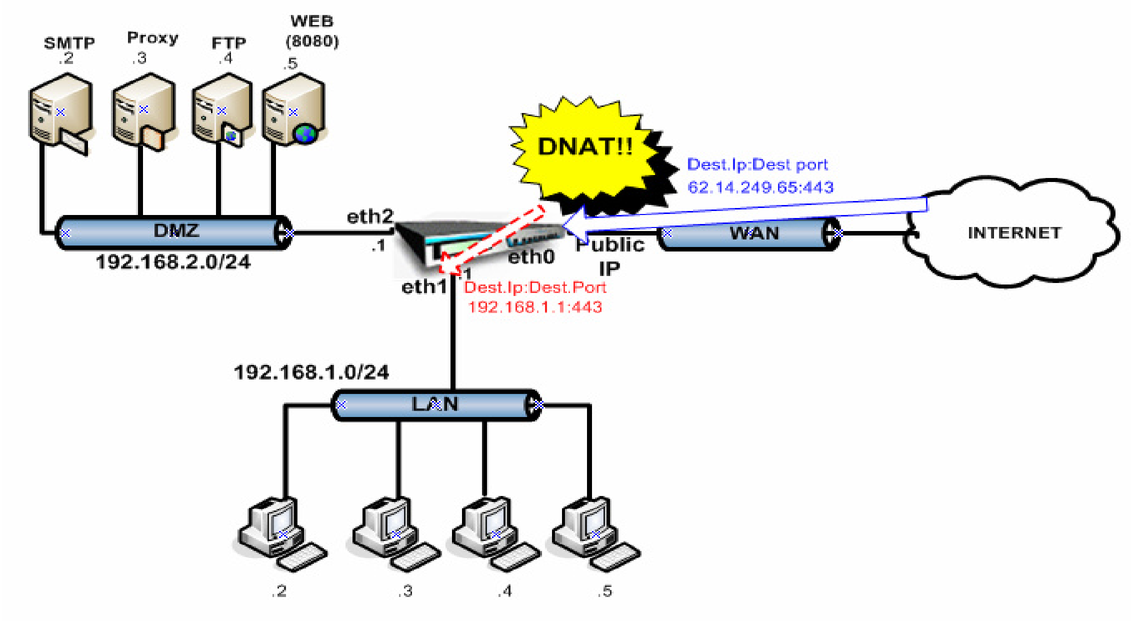
This means the only way of reaching both Integra and its internal networks (LAN and the DMZ in this case) is through the public IP address assigned to the machine.

2. Procedure

As can be seen in the previous illustration, access to the Web console is configured on the eth1 interface.

By entering a DNAT rule, it is possible, without changing the console settings, to access the Web console both from the eth1 and eth0 interfaces.

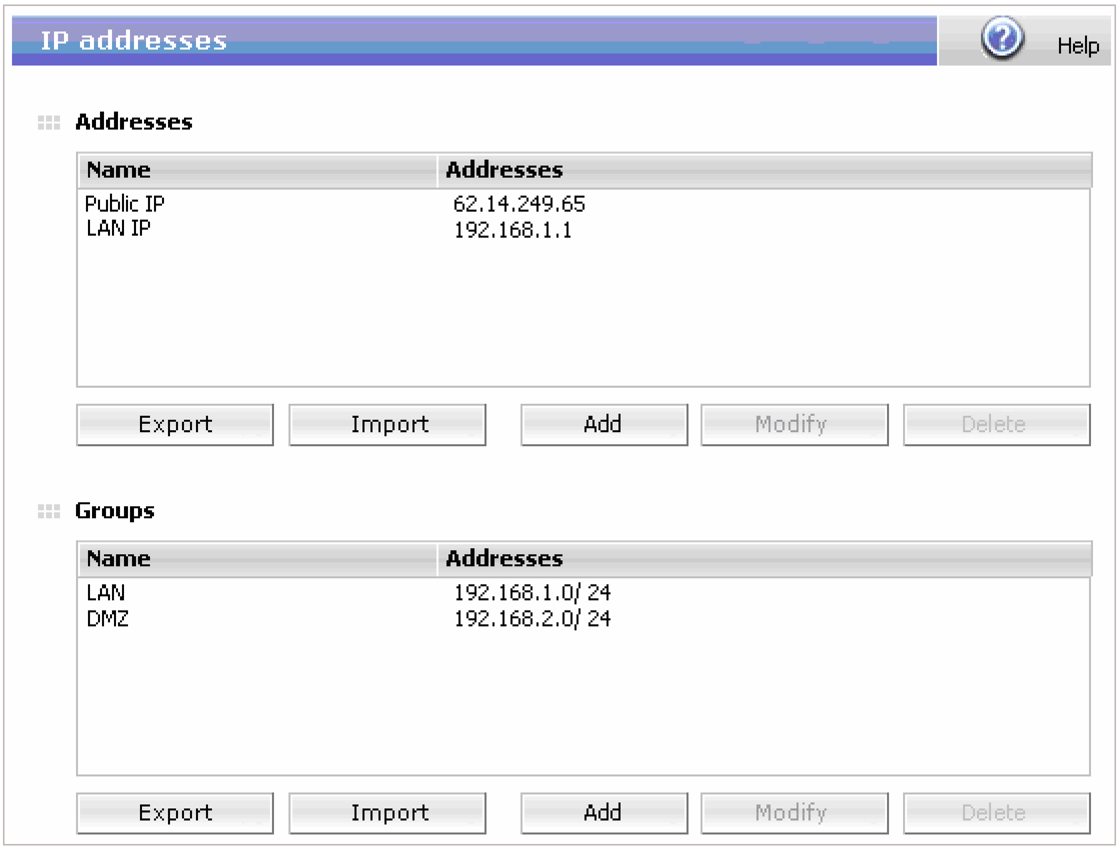
To do this and to map the HTTPS traffic in the eth0 interface towards the eth1 interface as if it were another corporate server offering external services, all you need to do is enter that rule.



With this configuration, requests to the Integra public IP address through port 443 will go through Integra, which will change the target IP address for the private IP address of the eth1 interface.

Follow the steps below according to the defined scenario:

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



IP addresses

Addresses

Name	Addresses
Public IP	62.14.249.65
LAN IP	192.168.1.1

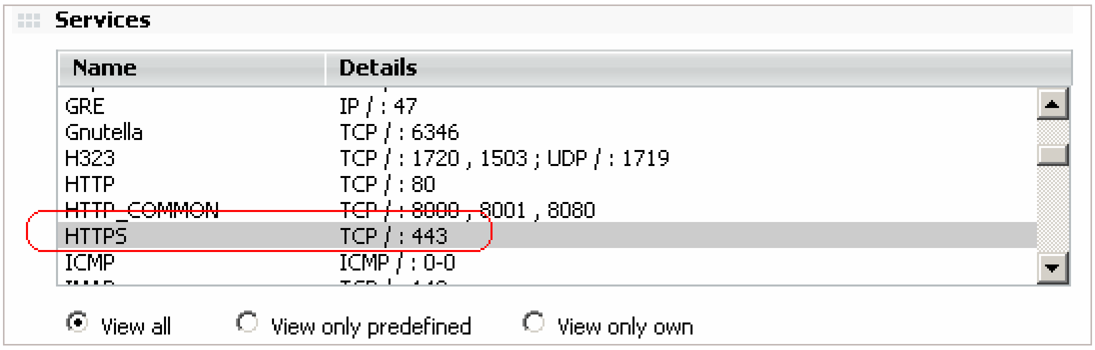
Groups

Name	Addresses
LAN	192.168.1.0/ 24
DMZ	192.168.2.0/ 24

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

Note: This step is not obligatory. You can enter the addresses without having previously defined them, although it simplifies the task when entering a lot of rules.

2. Define the service to be mapped. In this case it will not be necessary to add a new one as HTTPS in port 443 already exists in the predefined default services:



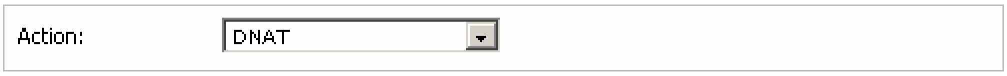
Services

Name	Details
GRE	IP / : 47
Gnutella	TCP / : 6346
H323	TCP / : 1720 , 1503 ; UDP / : 1719
HTTP	TCP / : 80
HTTP_COMMON	TCP / : 8000 , 8001 , 8080
HTTPS	TCP / : 443
ICMP	ICMP / : 0-0

● View all ○ View only predefined ○ View only own

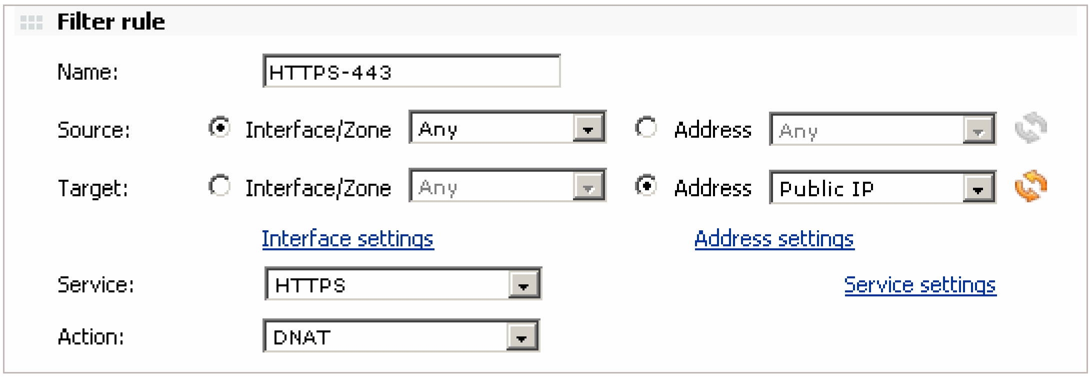
3. Add the DNAT rule that maps the HTTPS traffic through port 443 to the eth1 (LAN) interface:

Select DNAT as the action, which creates the DNAT rule:



Action: DNAT

Assign a name and define the characteristics of the traffic affected by the rule:



Filter rule

Name: HTTPS-443

Source: ● Interface/Zone Any ○ Address Any

Target: ○ Interface/Zone Any ● Address Public IP

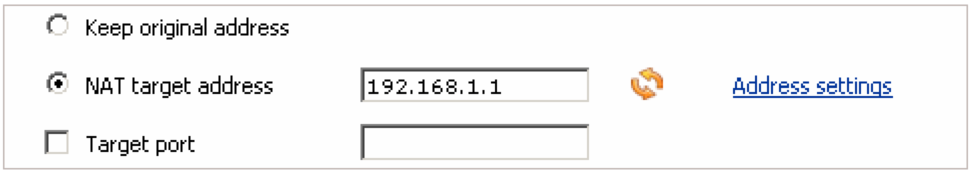
Interface settings Address settings

Service: HTTPS Service settings

Action: DNAT

- This will be applied to traffic from whatever source, as the source of requests from the Internet is unknown.
- The target should be the IP address of the interface to which traffic will be sent, in this case the Web interface with the public IP address assigned.
- The service for which this rule will be applied is, in this case, HTTPS, defined by default and which includes HTTPS traffic through port 443.

4. Define the parameters of the end target of the static mapping:



○ Keep original address

● NAT target address 192.168.1.1 Address settings

□ Target port

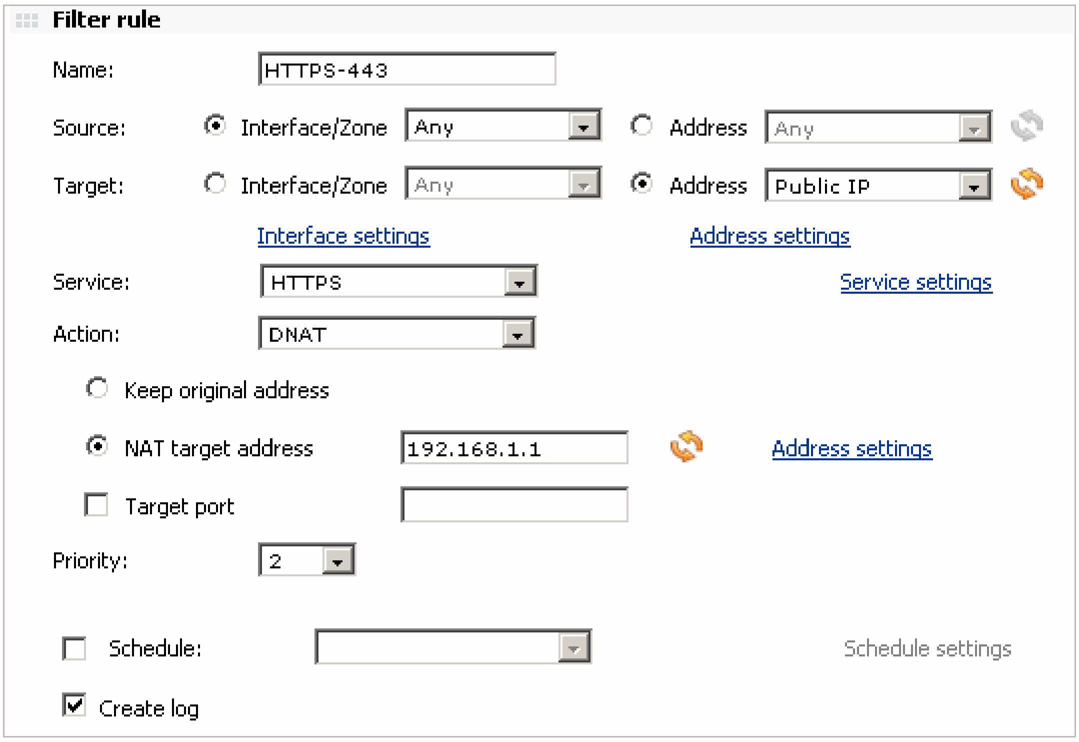
In the **NAT target address** field, enter the target server of the HTTPS request. In this case, you can use the definition entered for the eth1 interface IP address or manually enter the IP address of this interface, which in this case will act as the target server for the HTTPS request.

If the *Keep original address* option is enabled, the target header will not be modified. This can be used in special circumstances.

The *Target port* option in this case is not necessary as the target port will not change.

5. Define the rest of the optional information parameters, rule planning, etc.

Once all parameters are defined, the rule will be as illustrated below:



Filter rule

Name: HTTPS-443

Source: ● Interface/Zone: Any ○ Address: Any

Target: ○ Interface/Zone: Any ● Address: Public IP

Service: HTTPS

Action: DNAT

○ Keep original address

● NAT target address: 192.168.1.1

□ Target port

Priority: 2

□ Schedule:

☑ Create log

Once you have entered the DNAT rule, it is important that traffic which will be redirected is not blocked by the firewall filter rules.

In this case, there is already a rule to allow HTTPS traffic, so it will not be necessary to add another rule to allow this traffic.

0906-PGDIHT04-01-EN