Grandstream Networks, Inc.

GWN7000 - Firewall Features

Advanced NAT Configuration Guide

Table of Content

Table of Figures

INTRODUCTION

A firewall is a set of security measures designed to prevent unauthorized access to a networked computer system. It is like walls in a building construction, because in both cases their purpose is to isolate one "network" or "compartment" from another.

To protect private networks and individual machines from the dangers of Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called firewall policies. Firewall advanced settings on the GWN7000 is used to setup incoming/outgoing filter for WAN ports as well as setting up SNAT and DNAT.

Network Address Translation (NAT) technology, is described in RFC1631. Due to the growth of computers connected to the Internet, the pool of public IPv4 addresses was nearly exhausted. It was quickly realized that public IP addresses for the newly built networks would be very short. To remedy this, NAT was invented. NAT technology is the new approach for IP network, that allowed for years to extend many existing networks, instead of giving a public IPv4 address to each machine on the network, private IP addresses was attributed on a Local Area Network and to connect to internet, a public IPv4 is assigned to this network, NAT protocol, as its name stats handle the translation between public and private IPs.

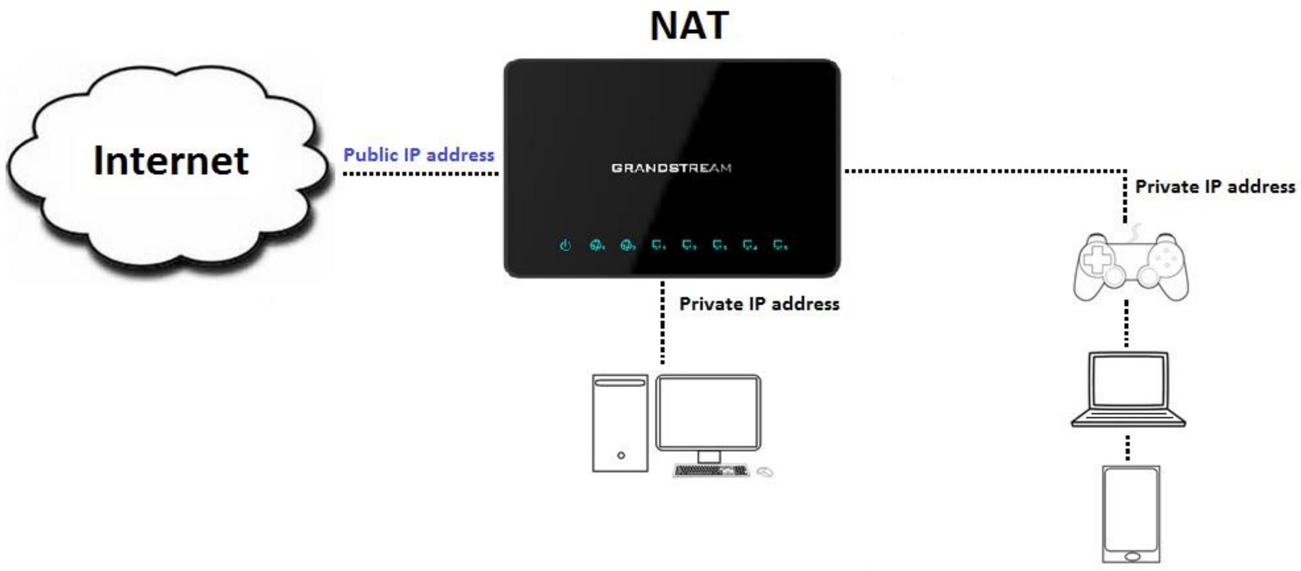


Figure 1: NAT Architecture

This guide will help you to understand and configure NAT advanced settings on GWN7000 series.
The configuration can be done from GWN7000 Web GUI > Firewall Advanced Settings page which provides ability to setup input/output policies for each WAN interface and Network Group; as well as setting configuration for Source and Destination NAT.

INPUT/OUPUT POLICIES

Overview

The Input/Output policy on the GWN7000 set configuration for WAN ports behavior when receiving/sending packets. It allows also to set limits on those ports and to enable MSS Clamping and IP Masquerading.

Below figure shows example of packets received by WAN2 port rejected while packets incoming from outside network to WAN1 are processed.

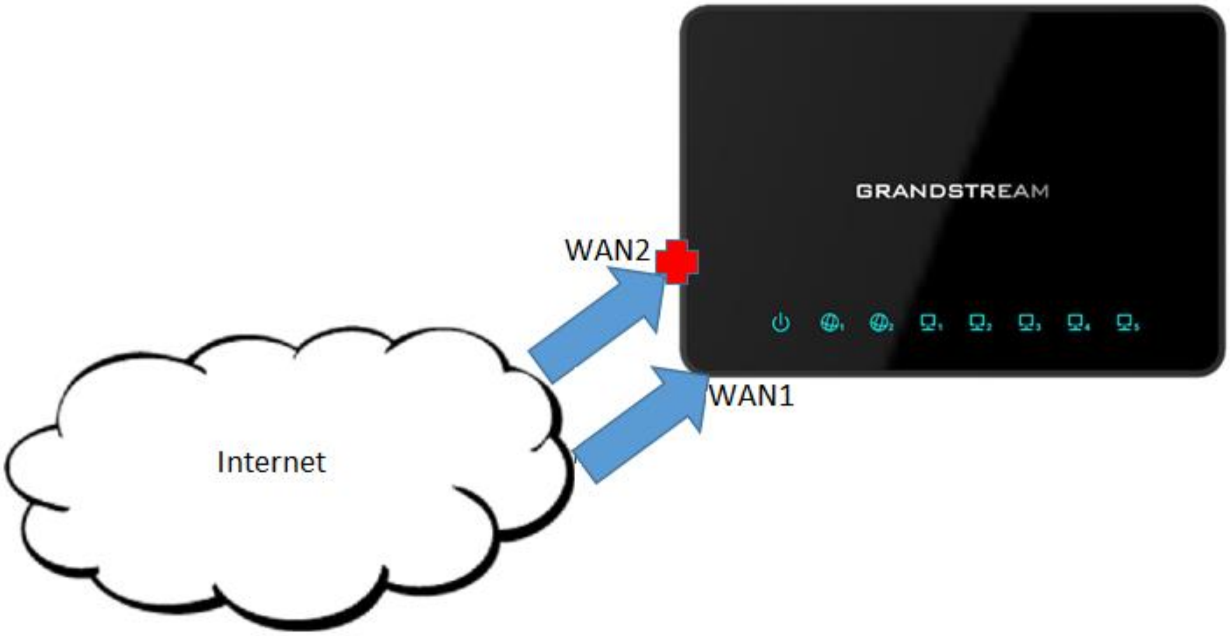


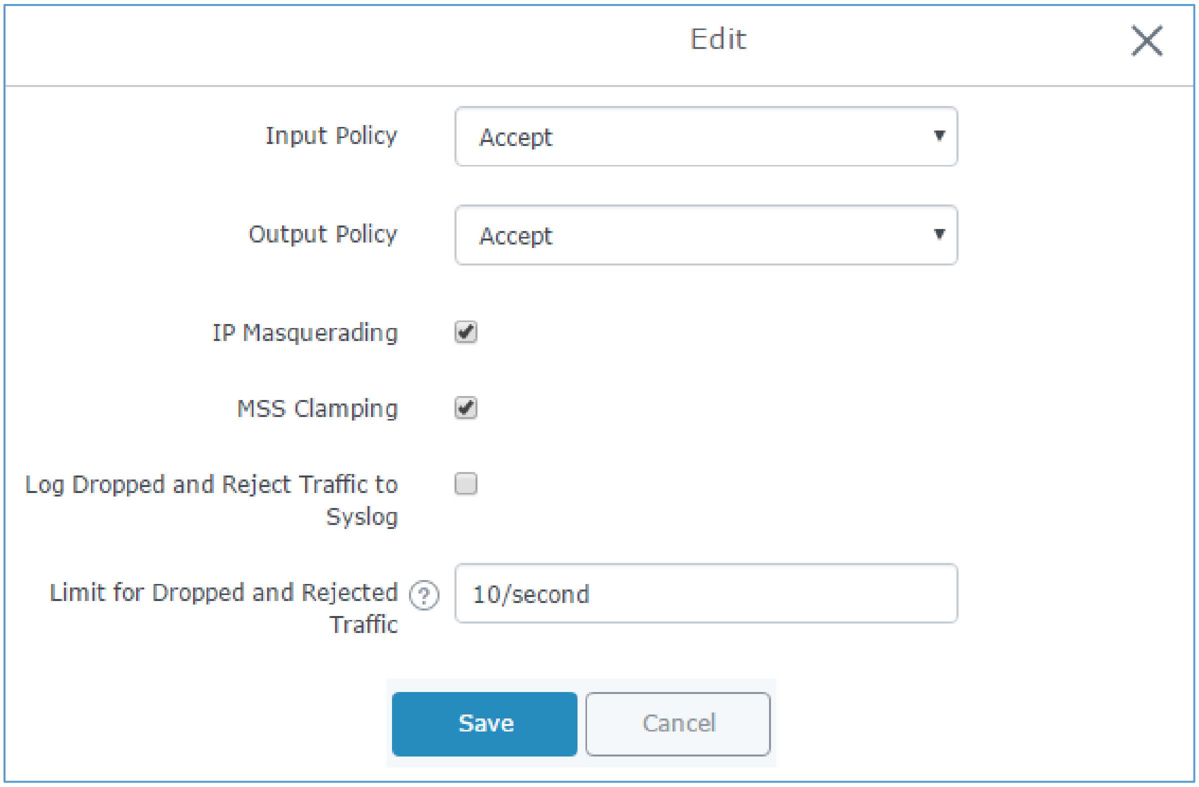
Figure 2: Input/Output Policy

Configuration

NAT input/output policies for each WAN interface or Network Groups can be configured from GWN7000 web GUI > Firewall > Advanced > General Settings.

An entry for each created/available network group or network interface can be found on this page, click on ✎ next to a WAN interface or Network group to edit its input and output policies.

The example below makes WAN port 1 accept any incoming traffic from outside the network.



Input Policy: Accept

Output Policy: Accept

IP Masquerading ☑

MSS Clamping ☑

Log Dropped and Reject Traffic to Syslog ☐

Limit for Dropped and Rejected Traffic: 10/second

Figure 3: General Settings

The following configuration was made on the above example:

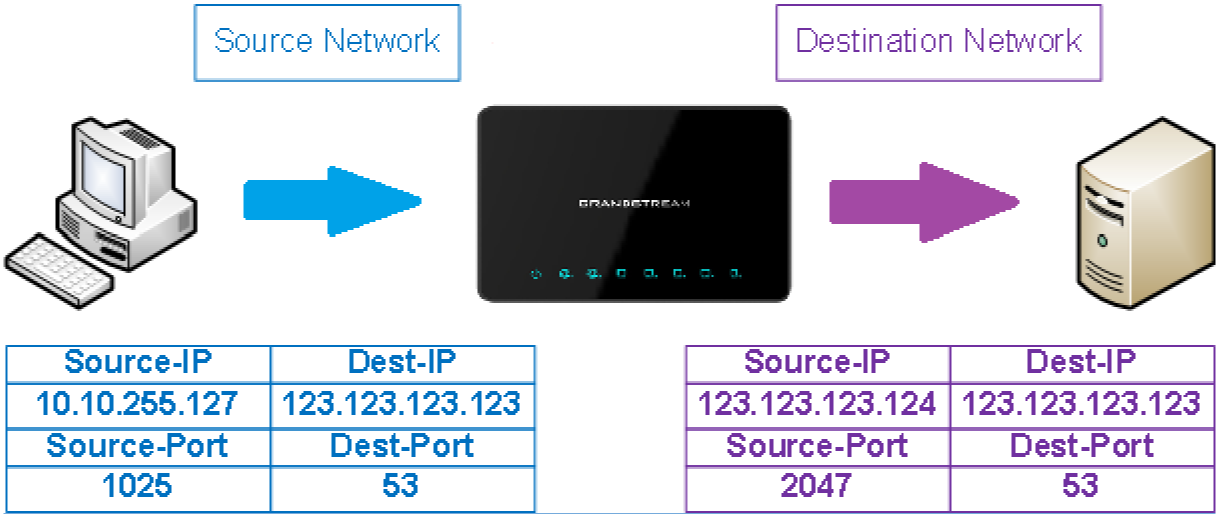
1. Select "Accept" from the "Input Policy" dropdown list so that any incoming packet to WAN port 1 will be accepted.
2. Select "Accept" from the "Output Policy" dropdown list so that any outgoing packet to from WAN port 1 will be accepted.
3. Check the "IP Masquerading" checkbox to allow internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
4. Check the "MSS Clamping" checkbox to provide a method to prevent fragmentation when the MTU value on the communication path is lower than the MSS value.
5. After filling the fields, click on Save ,then Apply to save and apply the settings.

By default, the "Input Policy" is reject which blocks access from WAN port to LAN, unless a port forwarding is set. This is not recommended as it allows unsecure network to access the GWN7000 LAN.

SNAT (SOURCE NAT)

Overview

The GWN7000 provides Source NAT feature, which changes the source address in IP header of a packet. It changes also the source port in the TCP/UDP headers. The typical usage is to change a private address/port into a public address/port for packets leaving the group or WAN port.



Source-IP	Dest-IP
10.10.255.127	123.123.123.123
Source-Port	Dest-Port
1025	53

Source-IP	Dest-IP
123.123.123.124	123.123.123.123
Source-Port	Dest-Port
2047	53

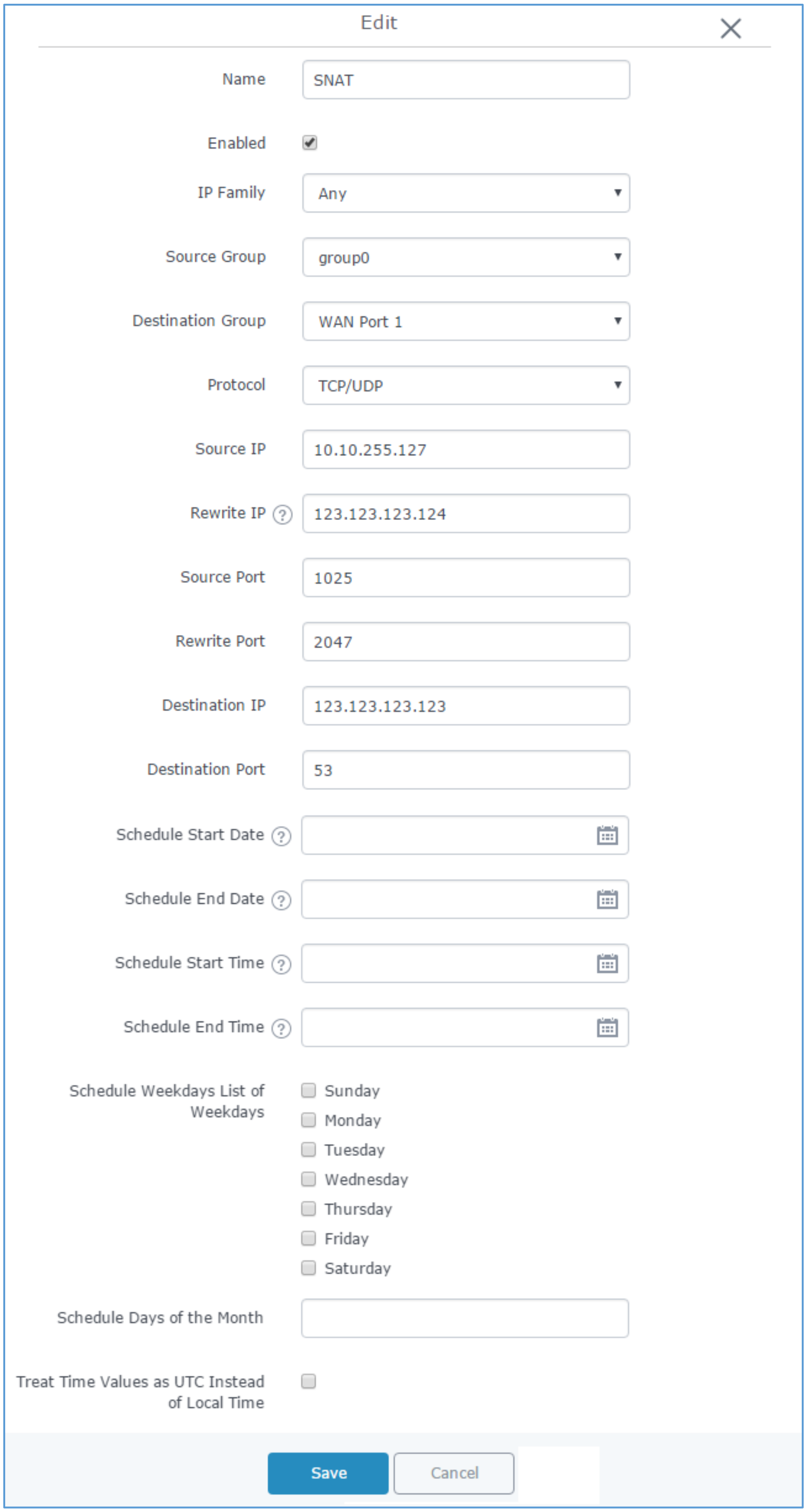
Figure 4: SNAT

Configuration

Following actions are available for SNAT from the GWN7000 web GUI under “Firewall > Advanced > SNAT”

- To add new SNAT entry, click on ⊕ Add
- To edit a SNAT entry, click on ✎
- To delete a SNAT rule, click on 🗑

Below figure provide an example of configuration for SNAT on the GWN7000.



Edit

Name	SNAT
Enabled	☑
IP Family	Any ▾
Source Group	group0 ▾
Destination Group	WAN Port 1 ▾
Protocol	TCP/UDP ▾
Source IP	10.10.255.127
Rewrite IP ?	123.123.123.124
Source Port	1025
Rewrite Port	2047
Destination IP	123.123.123.123
Destination Port	53
Schedule Start Date ?	
Schedule End Date ?	
Schedule Start Time ?	
Schedule End Time ?	
Schedule Weekdays List of Weekdays	□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
Schedule Days of the Month	
Treat Time Values as UTC Instead of Local Time	□

Figure 5: SNAT Example

The following configuration was made on the above example:

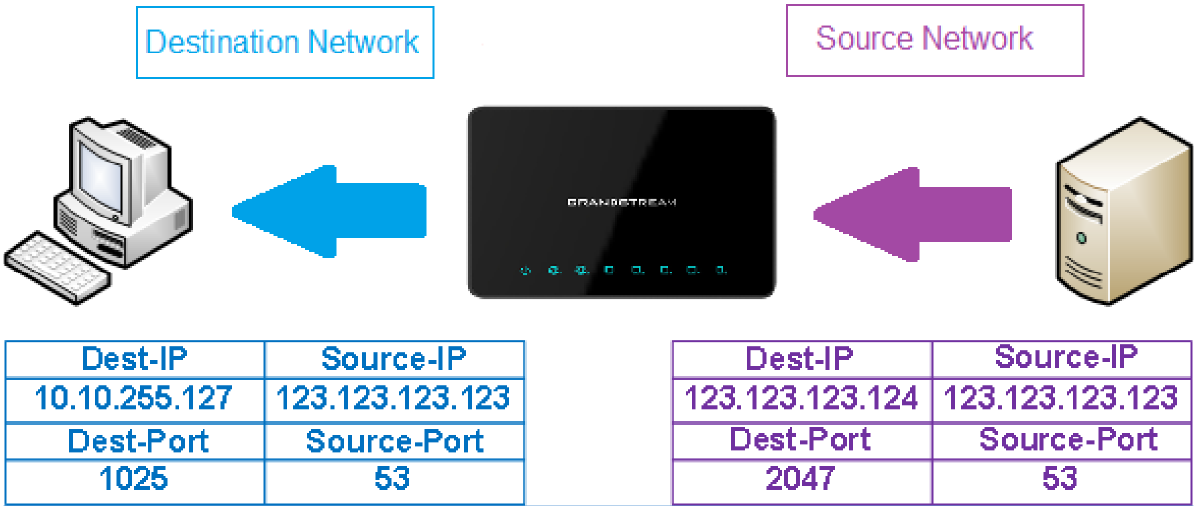
1. Specify a name to identify the SNAT rule.
2. Click on the “Enable” checkbox to enable the SNAT rule.
3. Select the IP version from the “IP Family” drop down list.
4. Select the source of incoming traffic from “Source Group” dropdown list, it could be an internal network group or external traffic from WAN port 1 or 2.
5. Select the Destination Group
6. Select one of the protocols from the “Protocol” dropdown list, available options are: UDP, TCP, TCP/UDP and All.
7. Enter the device Source IP.
8. Enter the IP that will go out from the GWN7000 to its destination on the “Rewrite IP”.
9. Enter the source port
10. Enter the rewrite port.
11. Enter the destination IP.
12. Enter the destination port.

For more details about other fields explanation please refer to NAT SETTINGS TABLE.

DNAT (DESTINATION NAT)

Overview

The GWN7000 allows users to configure Destination NAT or DNAT, which changes the destination address in IP header of a packet and change the destination port in the TCP/UDP headers. Typical usage of this is to redirect incoming packets with a destination of a public address/port to a private IP address/port inside your network.



Dest-IP	Source-IP
10.10.255.127	123.123.123.123
Dest-Port	Source-Port
1025	53

Dest-IP	Source-IP
123.123.123.124	123.123.123.123
Dest-Port	Source-Port
2047	53

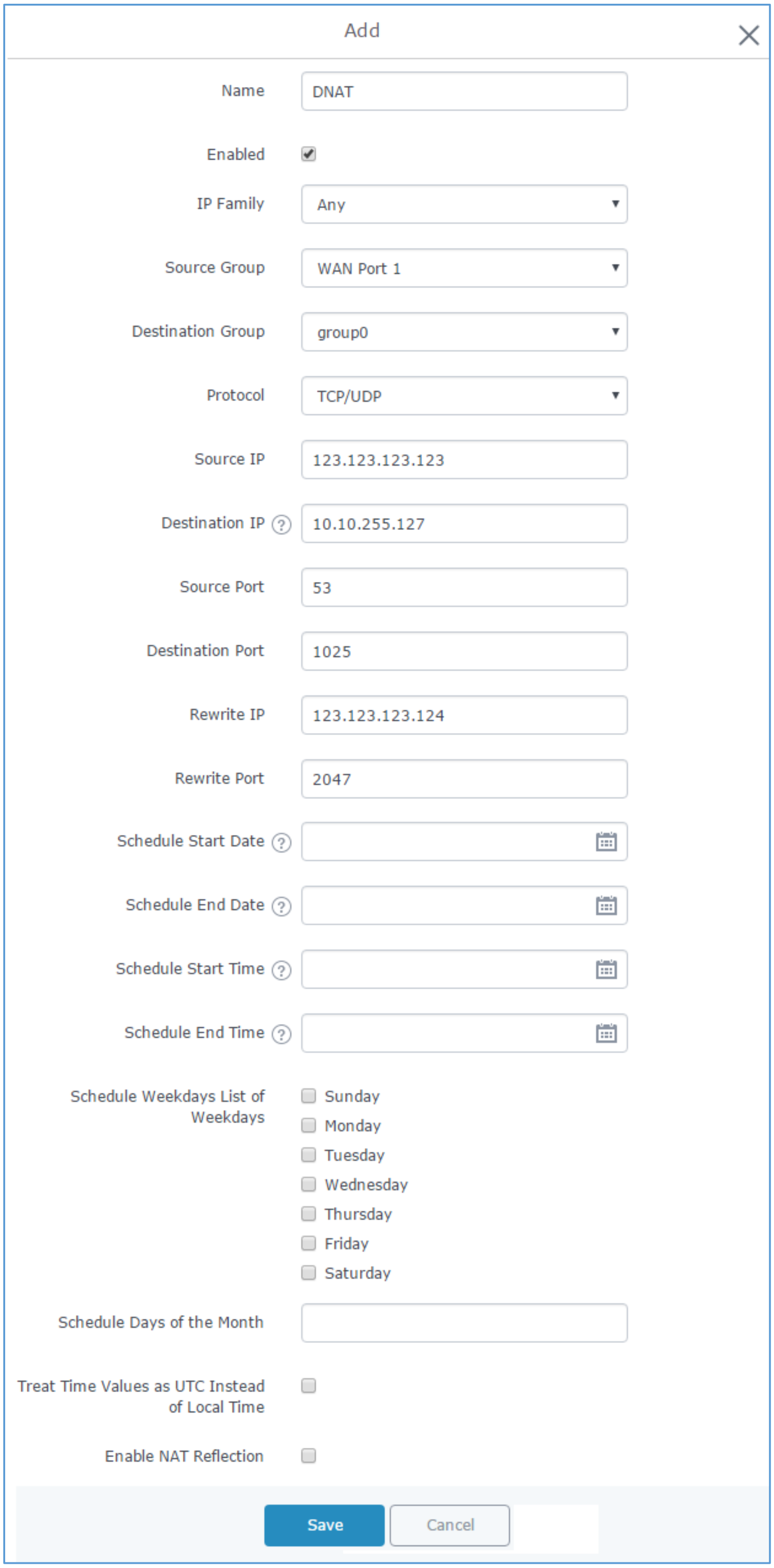
Figure 6: DNAT

Configuration

Following actions are available for DNAT from the GWN7000 web GUI under “Firewall > Advanced > DNAT”

- To add new DNAT entry, click on ⊕ Add
- To edit a DNAT entry, click on ✎
- To delete a DNAT rule, click on 🗑

Below figure provide an example of configuration for DNAT on the GWN7000.



Add

Name	DNAT
Enabled	☑
IP Family	Any
Source Group	WAN Port 1
Destination Group	group0
Protocol	TCP/UDP
Source IP	123.123.123.123
Destination IP	10.10.255.127
Source Port	53
Destination Port	1025
Rewrite IP	123.123.123.124
Rewrite Port	2047
Schedule Start Date	
Schedule End Date	
Schedule Start Time	
Schedule End Time	
Schedule Weekdays List of Weekdays	□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
Schedule Days of the Month	
Treat Time Values as UTC Instead of Local Time	□
Enable NAT Reflection	□

Figure 7: DNAT Example

The following configuration was made on the above example:

1. Specify a name to identify the SNAT rule.
2. Click on the “Enable” checkbox to enable the SNAT rule.
3. Select the IP version from the “IP Family” drop down list.
4. Select the source of incoming traffic from “Source Group” dropdown list, it could be an internal network group or external traffic from WAN port 1 or 2.
5. Select the Destination Group
6. Select one of the protocols from the “Protocol” dropdown list, available options are: UDP, TCP, TCP/UDP and All.
7. Enter the device Source IP.
8. Enter the destination IP.
9. Enter the source port
10. Enter the destination port.
11. Enter the IP that will go out from the GWN7000 to its destination on the “Rewrite IP”.
12. Enter the rewrite port.

For more details about other fields explanation please refer to NAT SETTINGS TABLE.

NAT SETTINGS TABLE

The following table provides explanation about all fields related to NAT configuration.

Field	Description
Name	Specify a name for the NAT entry
Enabled	Check to enable this NAT entry.
IP Family	Select the IP version. Three options are available: **IPv4**, **IPv6** or **Any**.
Source Group	Select a WAN interface or a LAN group for Source Group, or select All.
Destination Group	Select a WAN interface or a LAN group for Destination Group, or select All. Make sure that destination and source groups are different to avoid conflict.
Protocol	Select one of the protocols from dropdown list or All. Available options are: **UDP**, **TCP**, **TCP/UDP** and **All**.
Source IP	Set the Source IP address.
Rewrite IP	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
Destination IP	Set the Destination IP address.
Schedule Start Date	Click on 📅 icon to schedule a start date for this NAT entry to be applied.
Schedule End Date	Click on 📅 icon to schedule an end date for this NAT entry to end.
Schedule Start Time	Click on 📅 icon to schedule a start time for this NAT entry to be applied.
Schedule End Time	Click on 📅 icon to schedule an end time for this NAT entry to end.
Schedule Weekdays List of Weekdays	Select the days, on which the NAT entry will be applied, the unselected days will ignore this rule.
Schedule Days of the Month	Enter the days of the months (separated by space) on which the NAT entry will be applied. Example: **5 10 15** This will be applied only on 5th, 10th and 15th day monthly.
Treat Time Values as UTC Instead of Local Time	Check to use UTC as time zone for the specified times, instead of using GWN7000's local time.
Enable NAT Reflection	Check to enable NAT Reflection for this DNAT entry to allow the access of a service via the public IP address from inside the local network.