Grandstream Networks, Inc.

GWN7000 - Firewall Features

Traffic Rules 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.

Traffic Rules: Used to control incoming/outgoing, traffic in customized scheduled times, and taking actions for specified rules such as accept; reject and drop.

This guide will help you to understand and configure Traffic Rules features on the GWN7000.

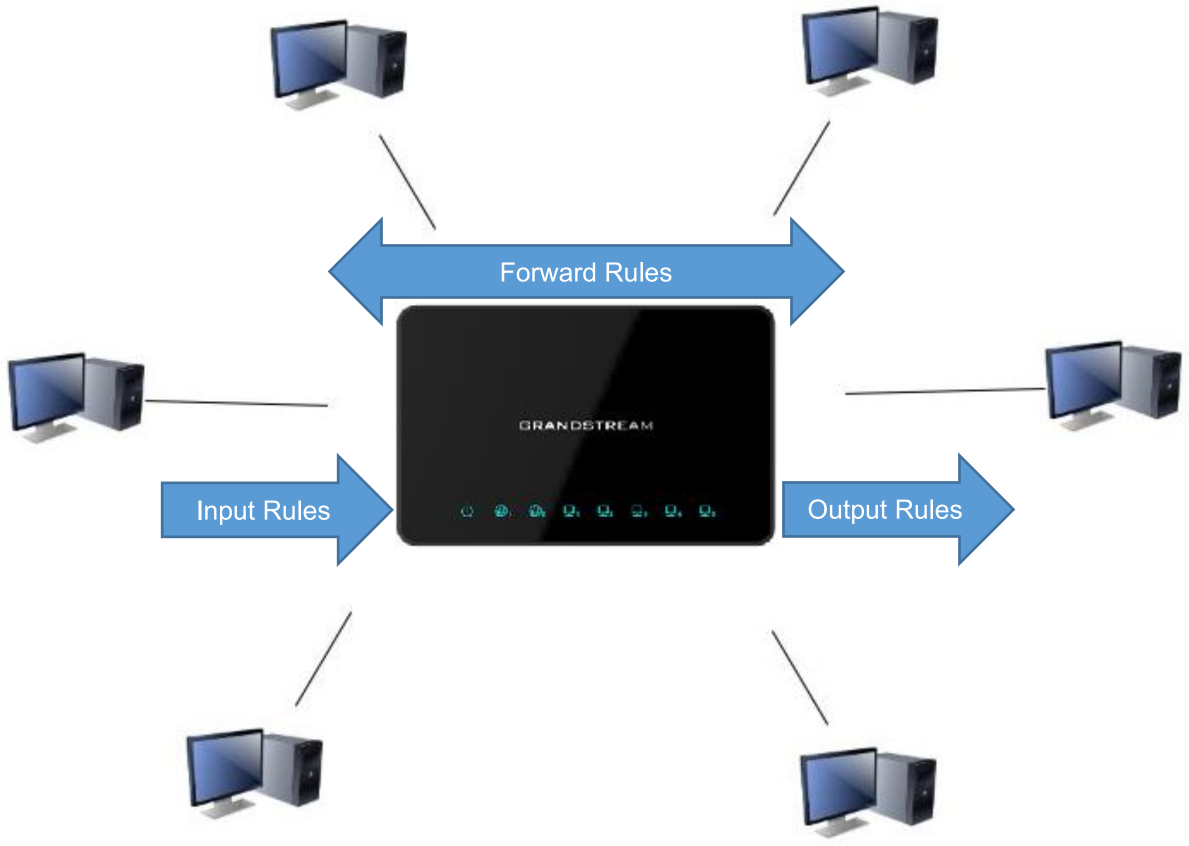


Figure 1: Firewall Architecture

TRAFFIC RULES

GWN7000 offers the possibility to fully control incoming/outgoing traffic for different protocols in customized scheduled times, and taking actions for specified rules such as Accept; Reject and Drop.

Input

The GWN7000 allows to filter incoming traffic to networks group or port WAN1 or WAN2 and apply rules such as:

- **Accept:** To allow the traffic to go through.
- **Reject:** A reply will be sent to the remote side stating that the packet is rejected.
- **Drop:** The packet will be dropped without any notice to the remote side.

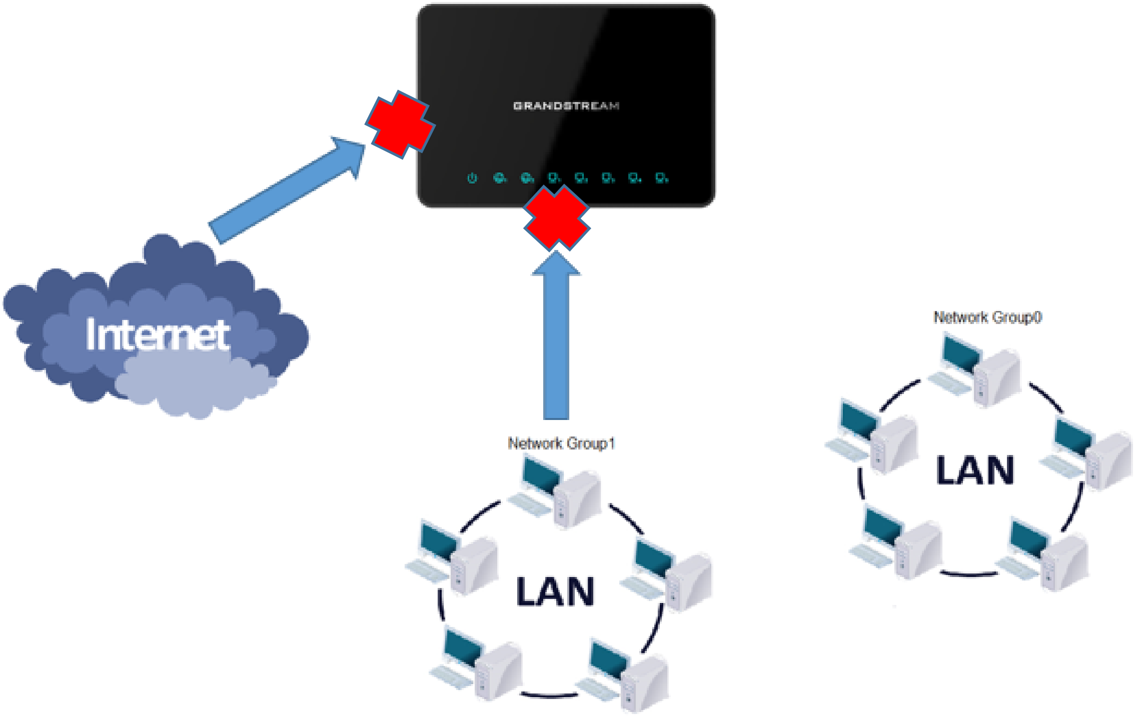


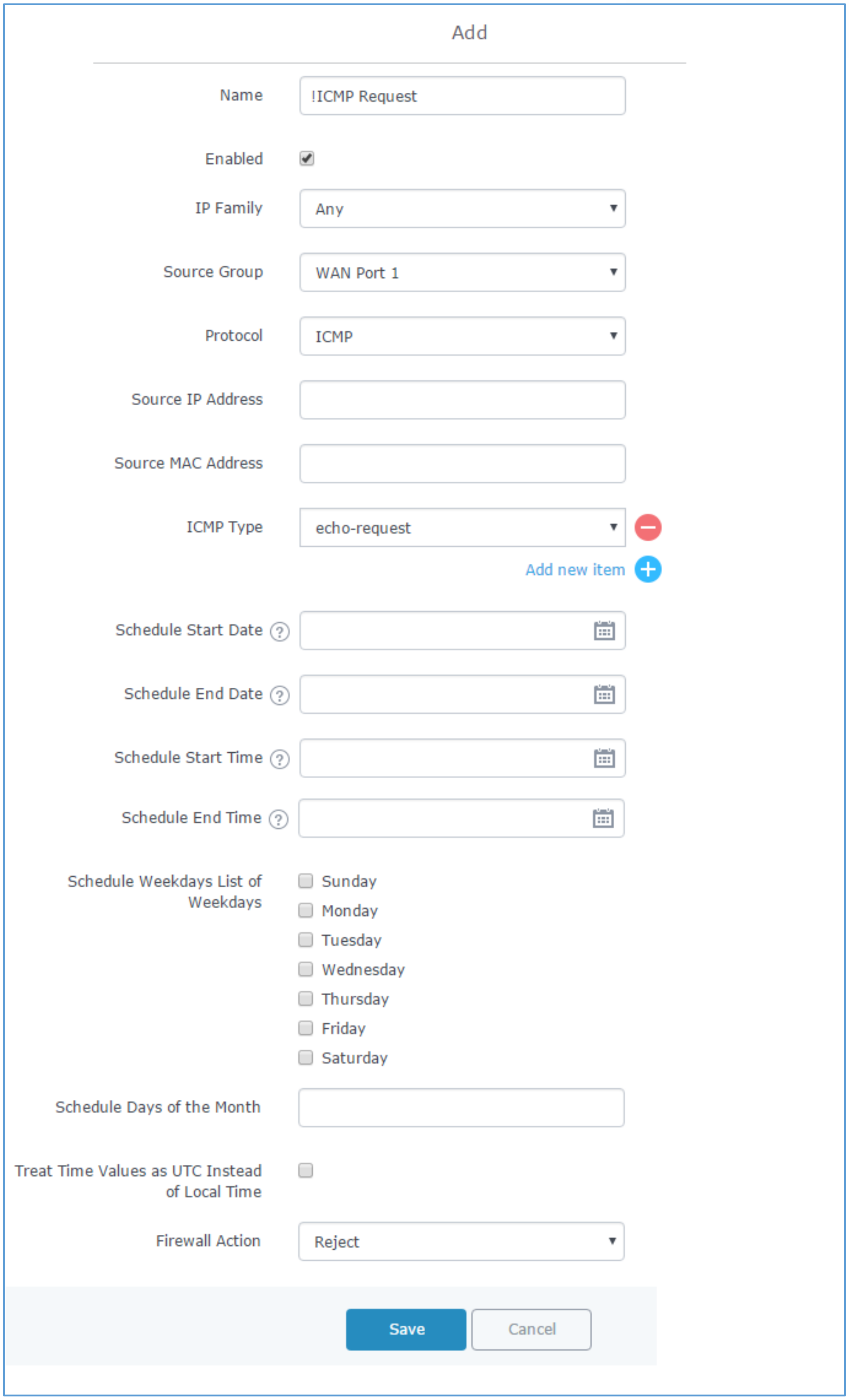
Figure 2: Input Traffic Rules

Following actions are available to configure Input rules on the GWN7000 under “Firewall > Traffic Riles > Input” for configured protocols.

- To add new rule, Click on ⊕ Add
- To edit a rule, Click on ✎
- To delete a rule, Click on 🗑

The following example rejects incoming ICMP request to WAN port 1, this means that whenever the GWN7000 receives and incoming ICMP request on WAN port 1 the destination IP address will receive a message stating that the destination IP address is unreachable.

Below screenshot shows configuration example:



Add

Name	!ICMP Request
Enabled	☑
IP Family	Any
Source Group	WAN Port 1
Protocol	ICMP
Source IP Address	
Source MAC Address	
ICMP Type	echo-request
	Add new item
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	□
Firewall Action	Reject

Figure 3: Input Rule ICMP Request Reject

1. Enter a name in the “Name” to identify the rule.
2. Click on “Enable” to activate the input rule.
3. Choose the IP version from “IP Family” whether it’s IPv4 or IPv6 or Any for both.
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. Choose the protocol you want to allow or reject.

   In this example: ICMP.
6. Select the protocol type you want to process.

   In our example: echo-request.
7. On the “Firewall Action” dropdown list chooses to allow, reject or drop.

   In our example: we selected reject so that incoming “echo-request” packets to the GWN7000 will be rejected.

For more details about other fields please refer to [TRAFFIC RULES TABLE].

Output

The GWN7000 allows to filter outgoing traffic from the local network group to outside networks and apply rules such as:

- **Accept:** To allow the traffic to go through.
- **Reject:** A reply will be sent to the remote side stating that the packet is rejected.
- **Drop:** The packet will be dropped without any notice to the remote side.

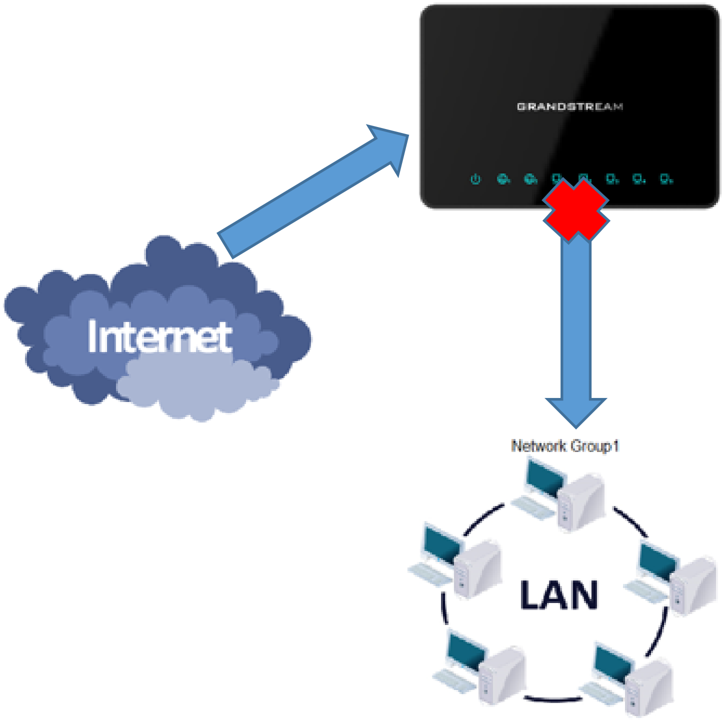


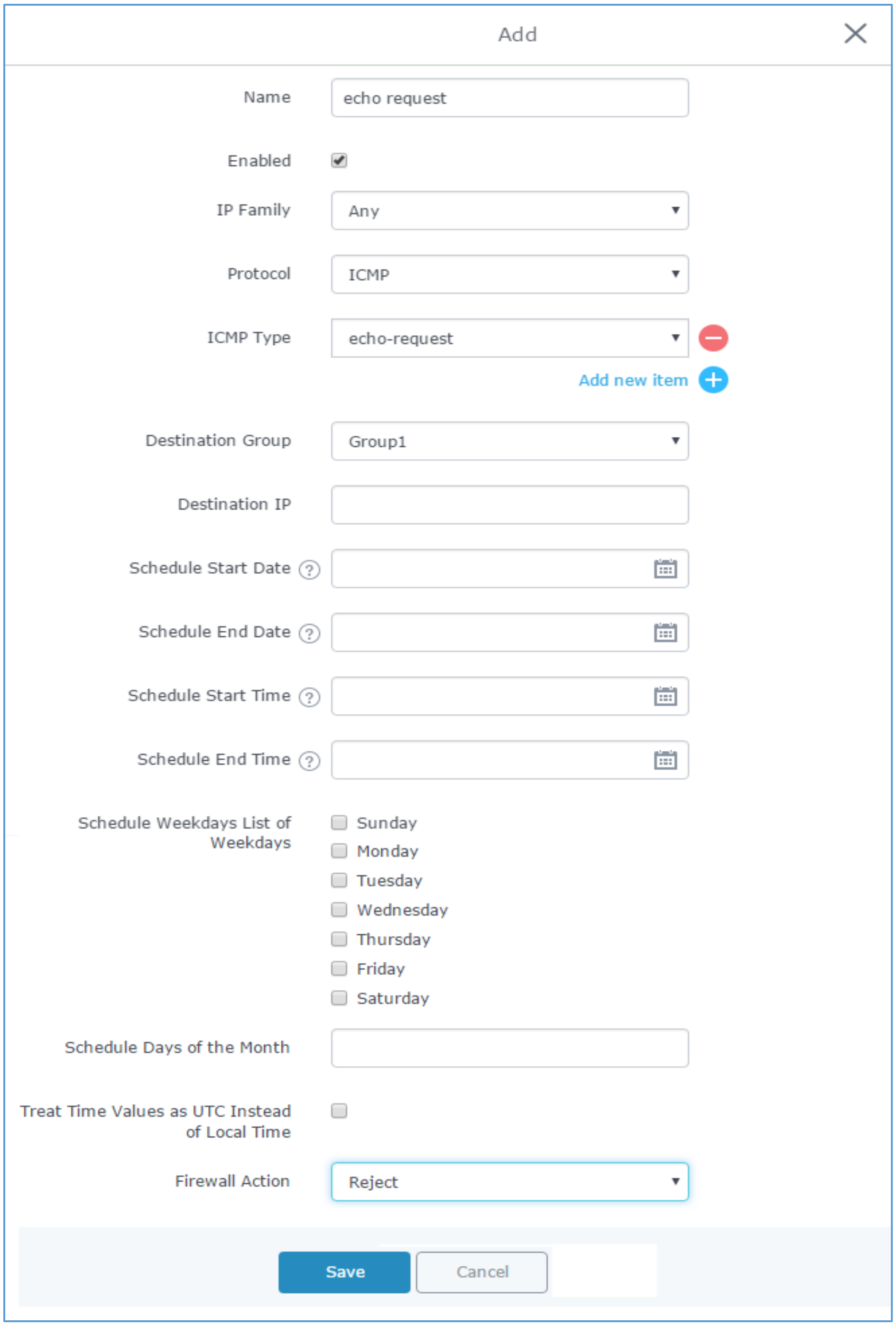
Figure 4: Output Traffic Rules

Following actions are available to configure Output rules on the GWN7000 under "Firewall > Traffic Riles > Output" for configured protocols.

- To add new rule, Click on ⊕ Add
- To edit a rule, Click on ✎
- To delete a rule, Click on 🗑

The following example will reject every outgoing ICMP request from GWN7000 to network Group1, this means that whenever the GWN7000 receives an ICMP "echo-request" from another network group or from WAN port 1 or 2 sent to network group 1 will be rejected.

Below screenshot shows configuration example:



Add

Name: echo request

Enabled: ☑

IP Family: Any

Protocol: ICMP

ICMP Type: echo-request

Destination Group: Group1

Destination IP:

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: □

Firewall Action: Reject

Figure 5: Output Rule ICMP Request Reject

1. Enter a name in the “Name” to identify the rule.
2. Click on “Enable” to activate the output rule.
3. Choose the IP version from “IP Family” whether IPv4 or IPv6 or Any for both.
4. Choose the protocol you want to allow or reject.

   <u>In this example:</u> ICMP.

5. Select the protocol type you want to process.

   In this example: echo-request.

6. Select the Destination Group

7. On the “Firewall Action” dropdown list chooses to allow, reject or drop.

   In this example: we selected reject so that incoming “echo-request” packets to the GWN7000 will be rejected.

For more details about other fields please refer to [TRAFFIC RULES TABLE].

Forward

The GWN7000 allows to filter traffic passing through it, from a group or a WAN port to another one and apply rules such as:

- **Accept:** To allow the traffic to go trough
- **Reject:** A reply will be sent to the remote side stating that the packet is rejected.
- **Drop:** The packet will be dropped without any notice to the remote side.

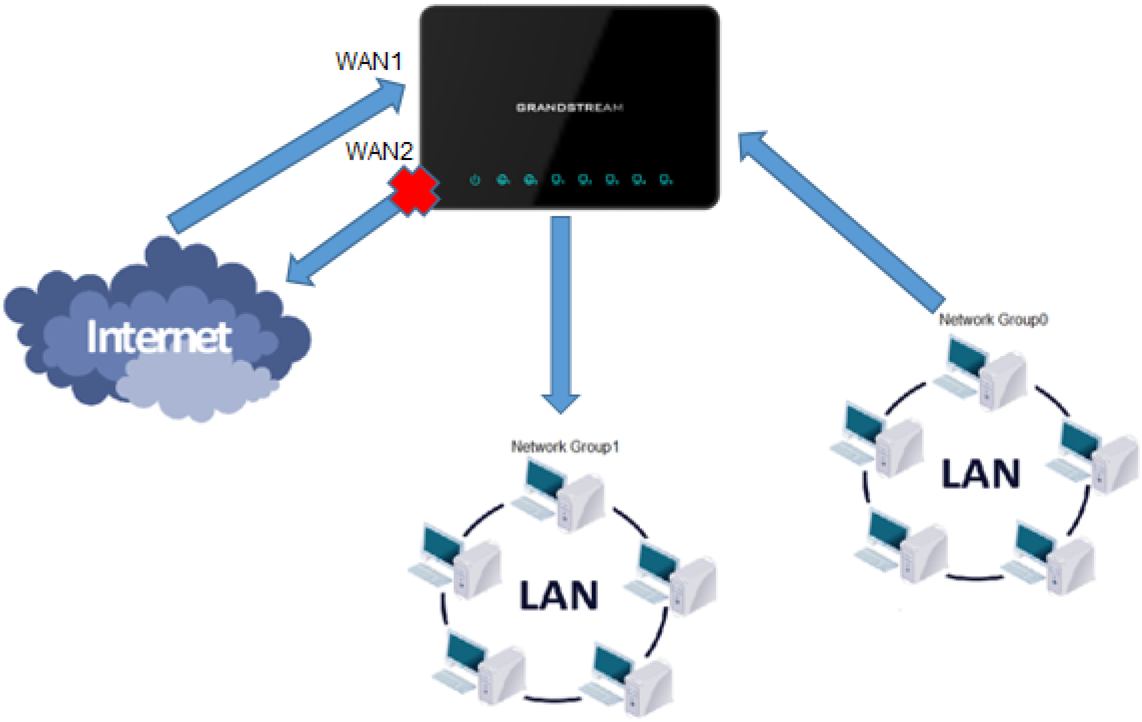


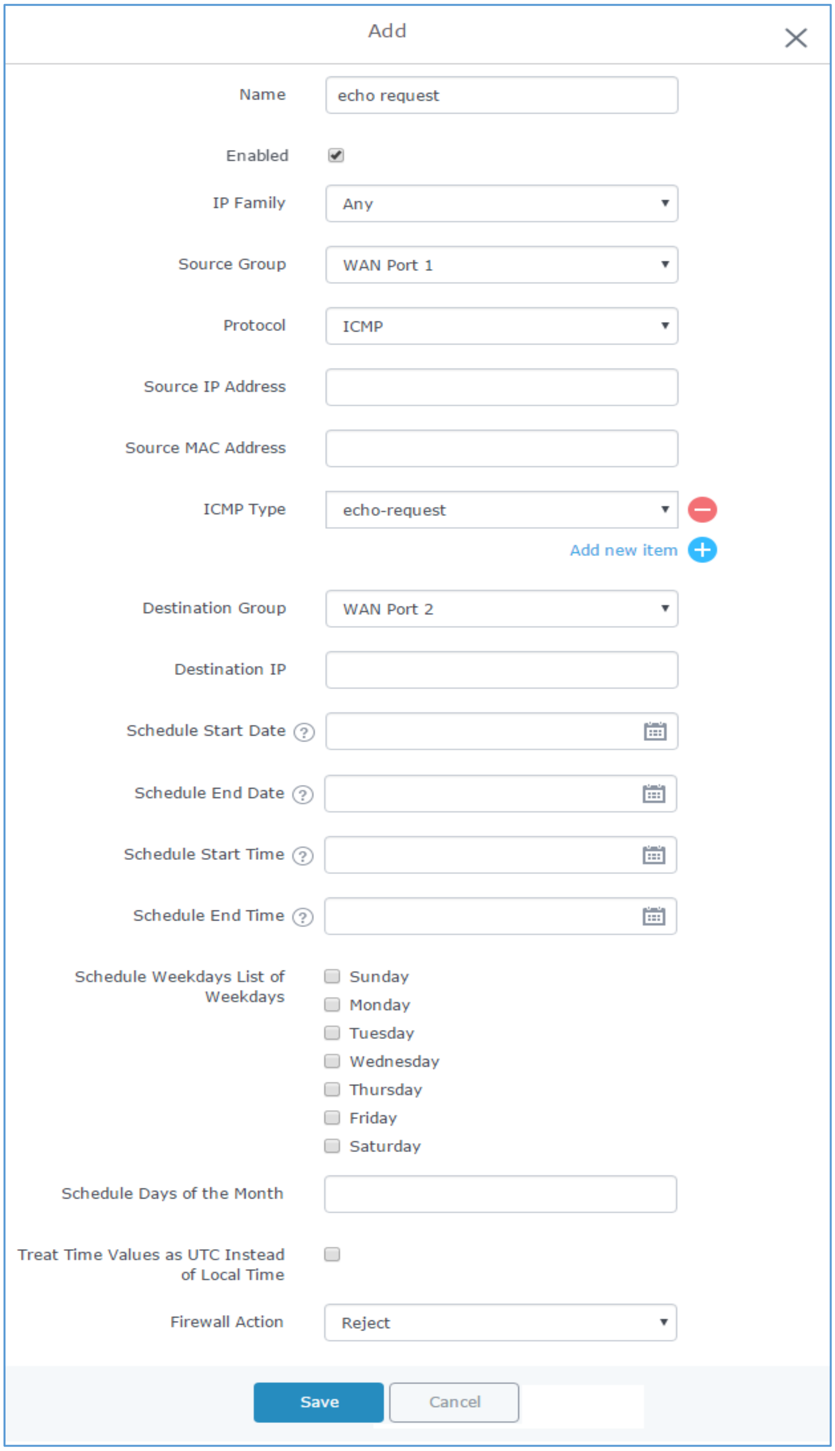
Figure 6: Forward Traffic Rules

Following actions are available to configure Forward rules on the GWN7000 under “Firewall > Traffic Riles > Forward” for configured protocols.

- To add new rule, Click on ⊕ Add
- To edit a rule, Click on ✎
- To delete a rule, Click on 🗑

The following example will reject every incoming ICMP request from WAN port 1 that has for destination WAN port 2, this means that whenever there is an ICMP “echo-request” passing through the GWN7000 from WAN port 1 to WAN port 2 the GWN700 will reject this packet.

Below screenshot shows configuration example:



Add

Name	echo request
Enabled	☑
IP Family	Any
Source Group	WAN Port 1
Protocol	ICMP
Source IP Address	
Source MAC Address	
ICMP Type	echo-request
Destination Group	WAN Port 2
Destination IP	
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	□
Firewall Action	Reject

Figure 7: Forward Rule ICMP Request Reject

1. Enter a name in the “Name” to identify the rule.
2. Click on “Enable” to activate the forward rule.
3. Choose the IP version from “IP Family” whether IPv4 or IPv6 or Any for both.
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. Choose the protocol you want to allow or reject.

   In this example: ICMP.
6. Select the protocol type you want to process.

   In this example: echo-request.
7. Select the Destination Group
8. On the “Firewall Action” dropdown list chooses to allow, reject or drop, in our example we selected reject so that incoming “echo-request” packets to the GWN7000 will be rejected.

For more details about other fields please refer to [TRAFFIC RULES TABLE].

TRAFFIC RULES TABLE

The following table provides explanation about each field related to traffic rules feature.

Field	Description
Name	Specify a name for the traffic rule.
Enabled	Check to enable this rule.
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.
Protocol	Select one of the protocols from dropdown list or All. Available options are: **UDP**, **TCP**, **TCP/UDP**, **UDP-Lite**, **ICMP**, **AH**, **SCTP**, **IGMP** and **All**.
Source IP Address	Set the source IP address. It can be an IPv4 or IPv6 address.
Source Port(s)	Set the source port. It can be one or many ports separated by spaces.
Source MAC address	Set the source MAC address.
Destination Port(s)	Set the destination port. It can be one or many ports separated by spaces.
Schedule Start Date	Click on 📅 icon to schedule a start date for this rule to be applied.
Schedule End Date	Click on 📅 icon to schedule an end date for this rule to cease effect.
Schedule Start Time	Click on 📅 icon to schedule a start time for this rule to be applied.
Schedule End Time	Click on 📅 icon to schedule an end time for this rule to cease effect.
Schedule Weekdays List of Weekdays	Select the days when the traffic rule will be applied. Unselected days will ignore this rule.
Schedule Days of the Month	Enter the days of the months (separated by space) when the traffic rule 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.
Firewall Action	Select which action to perform for the given traffic rule. Three options are available: **Accept**, **Reject** or **Drop**.