Grandstream Networks, Inc.

Grandstream Routers

Firewall Traffic Rules Guide

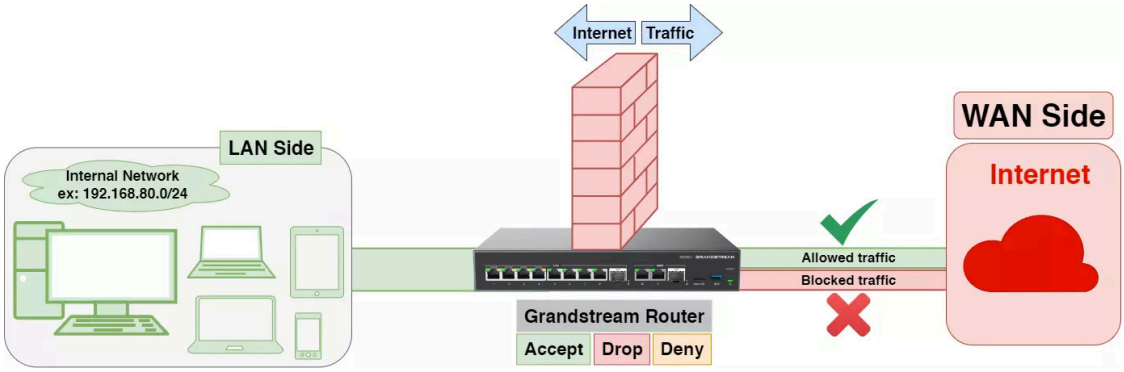
OVERVIEW

A firewall is a set of security measures designed to prevent unauthorized access to a networked computer system. It is similar to building walls in that their purpose is to separate one “network” or “compartment” from another.

To protect private networks and individual machines from the dangers of the 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 take actions for specified rules such as accept, reject and drop.

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



Firewall Traffic Rules Diagram

TRAFFIC RULES

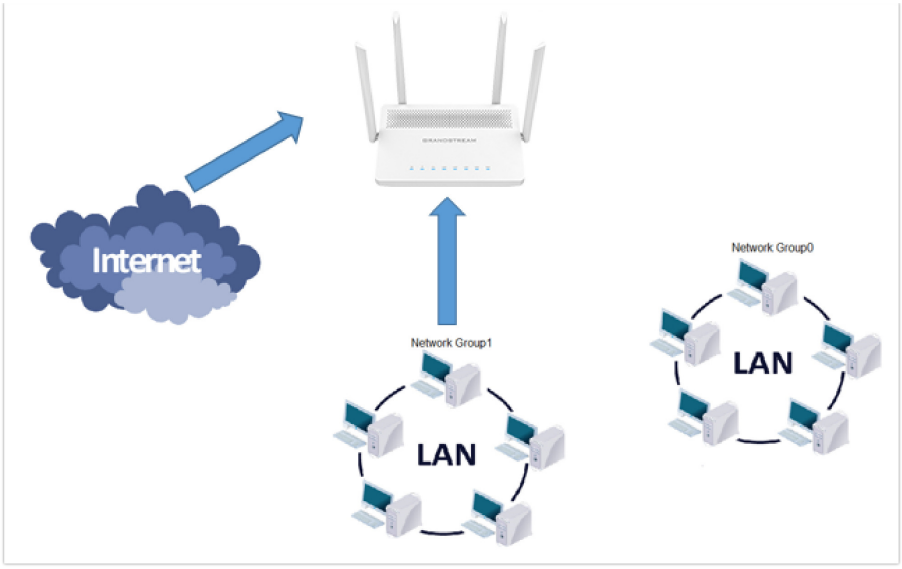
Grandstream routers offer the possibility to fully control incoming/outgoing traffic for different protocols in customized scheduled times, and take actions for specified rules such as Accept, Reject, and Drop.

Inbound Rules

Inbound traffic rules are used to control the traffic that is coming into the router from external networks or devices. These rules can be used to restrict access to certain services or ports, block traffic from specific IP addresses or ranges, or allow traffic from trusted sources. For example, an inbound traffic rule may allow incoming traffic on port 80 (HTTP) to a web server hosted behind the router, while blocking all other incoming traffic.

The router allows to filter of incoming traffic to network group or port WAN1 or WAN2 and applies rules such as:

- **Accept:** To allow the traffic to go through.
- **Deny:** 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.

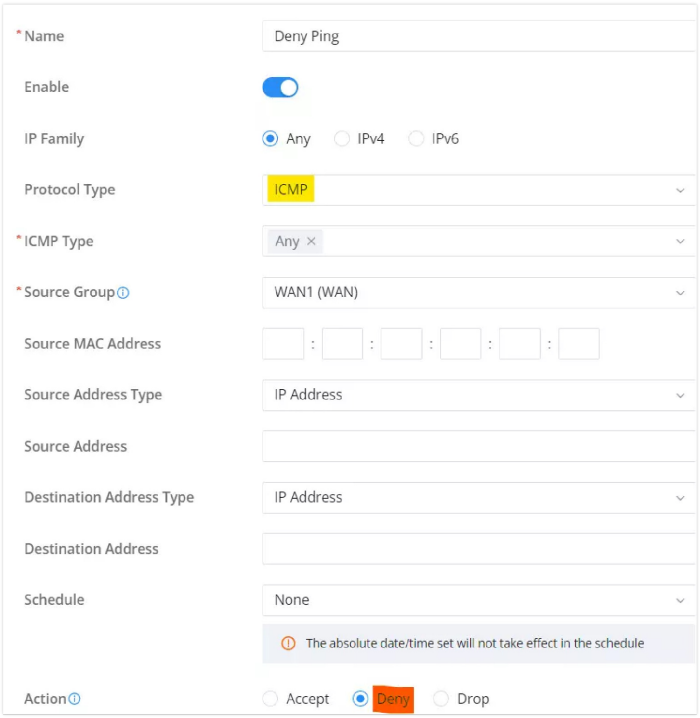


Inbound Rules Diagram

The previous actions are available to configure inbound rules on the router under "Firewall →Traffic Rules → Input" for configured protocols.

The below example shows the configuration steps done to create an Inbound Traffic rule :

1. Navigate to "**Firewall→ Traffic Rules**".
2. On the **Inbound Rules** Tab, Click on the "**Add**" button to create a new rule.*
3. Enable the rule (Status ON), Source Group (WAN), and protocol type (in our case it's ICMP and ICMP type = Any), and the Action is **Deny**.



4. Open the command prompt or terminal then ping the router (WAN port IP Address) before adding the inbound rule and after adding the inbound rule.

Before adding the Inbound rule

```
C:\Users\Jawad>ping 192.168.5.55

Pinging 192.168.5.55 with 32 bytes of data:
Reply from 192.168.5.55: bytes=32 time<1ms TTL=64
Reply from 192.168.5.55: bytes=32 time<1ms TTL=64
Reply from 192.168.5.55: bytes=32 time<1ms TTL=64
Reply from 192.168.5.55: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.5.55:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

After adding the Inbound rule

```
C:\Users\Jawad>ping 192.168.5.55

Pinging 192.168.5.55 with 32 bytes of data:
Reply from 192.168.5.55: Destination port unreachable.
Reply from 192.168.5.55: Destination port unreachable.
Reply from 192.168.5.55: Destination port unreachable.
Reply from 192.168.5.55: Destination port unreachable.
```

> **Note**
>
> If traffic flows from LAN-side to WAN-side, then the traffic is outbound. If the traffic flows from WAN-side to LAN-side, then the traffic is inbound.

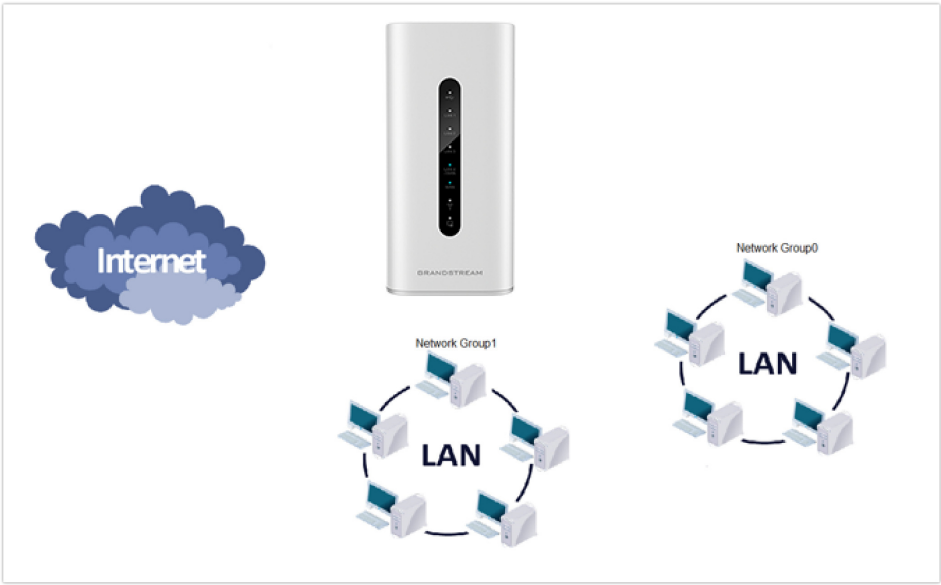
For more details about other fields please refer to [TRAFFIC RULES TABLE].

Outbound Rules

Outbound traffic rules are used to control the traffic that is leaving the router and going to external networks or devices. These rules can be used to restrict access to certain services or ports, block traffic to specific IP addresses or ranges, or allow traffic to trusted sources. For example, an outbound traffic rule may allow outgoing traffic on port 443 (HTTPS) to a secure website, while blocking all other outgoing traffic.

The router allows to filter of outgoing traffic from the local network group to outside networks and applies rules such as:

- **Accept:** To allow the traffic to go through.
- **Deny:** 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.

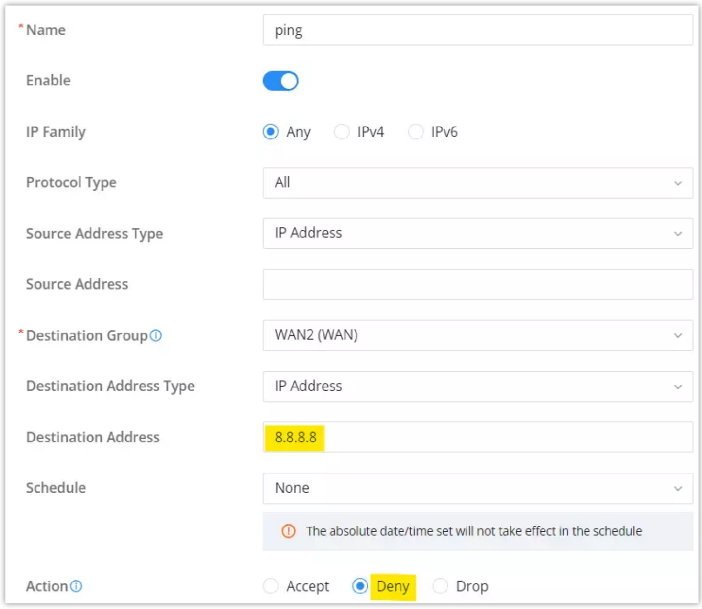


Outbound Rules Diagram

In the following example, we show how to create an Outbound Traffic rule:

1. Navigate to "**Firewall→ Traffic Rules**".

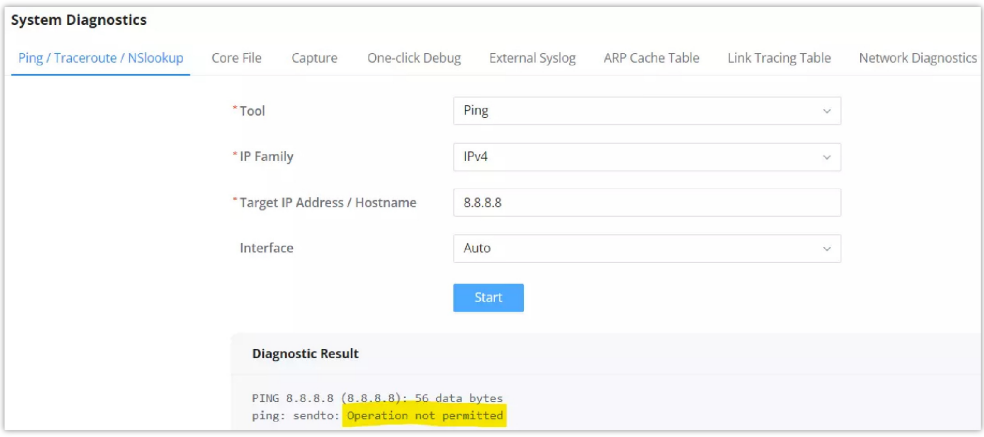
2. On the Outbound Rules Tab, Click on the "**Add**" button to create a new rule.
3. Enable the rule (**Status ON**), Destination Group (**WAN**), and Destination IP (in our case it's the DNS **8.8.8.8**) and the Action is **Deny**.



DNS Rule

4. To verify the Outbound rule, the Grandstream routers have a built-in **Ping/Traceroute** tool for troubleshooting purposes.

5. Select the IP Address (ex: **8.8.8.8**) then the interface (**WAN**) and click the button "**Start**". The expected result is **"Operation not permitted".**



Outbound Rule Ping Test example

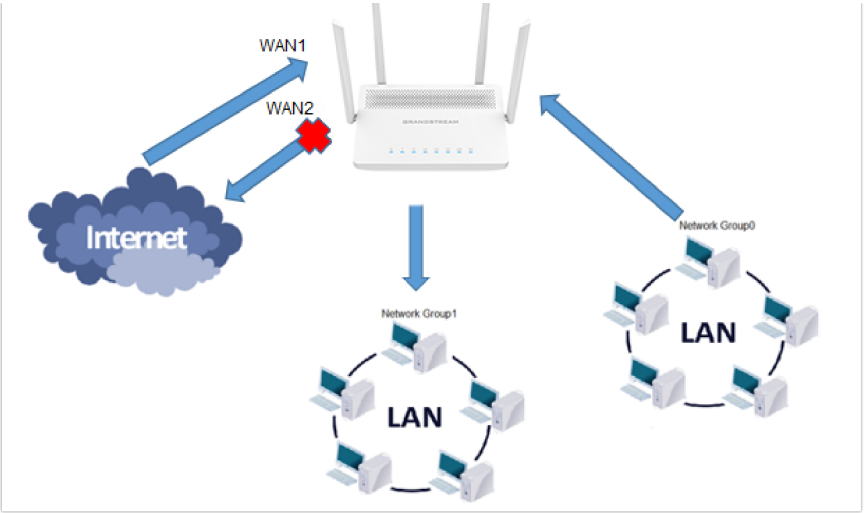
For more details about other fields please refer to [TRAFFIC RULES TABLE].

Forwarding Rules

The Forwarding rules are used to control the traffic that is being forwarded between different networks or devices within the network. The purpose of forwarding traffic rules is to direct traffic to the appropriate destination based on the network topology and the type of traffic. Forwarding traffic rules can be used to specify the next hop for the traffic, based on the destination IP address or network, the type of protocol used (TCP, UDP, ICMP), or the port number. For example, a forwarding traffic rule may direct incoming traffic from a specific subnet to a particular server on the network.

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

- **Accept:** To allow the traffic to go trough
- **Deny:** 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.

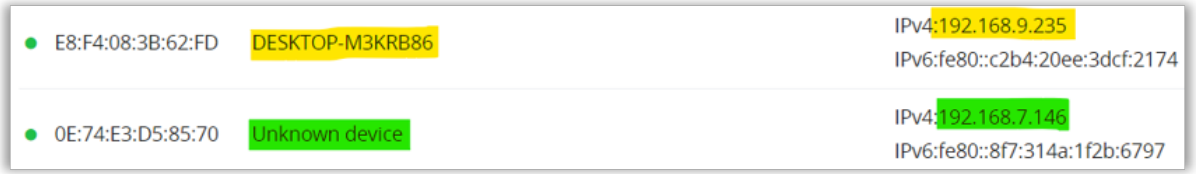


Forwarding rule Diagram

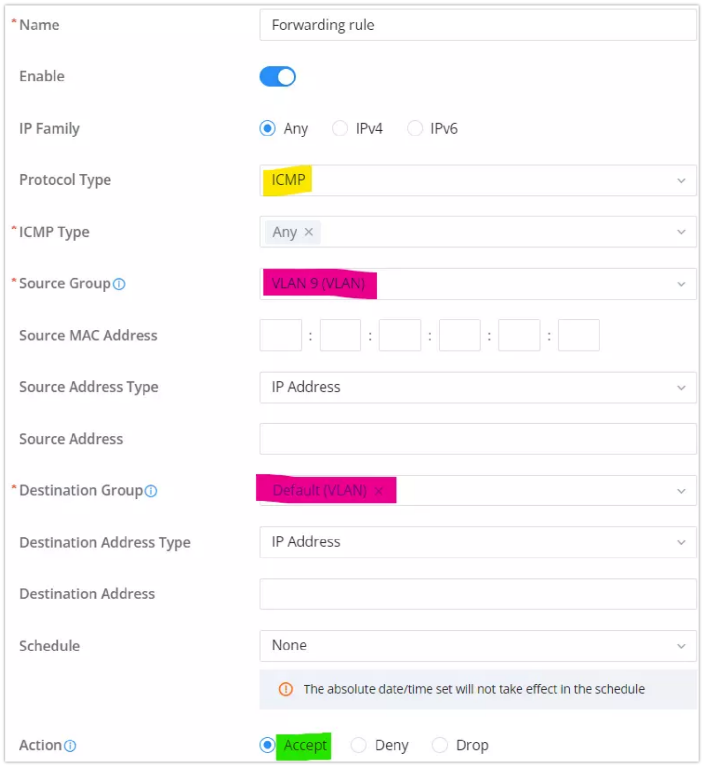
The following actions are available to configure Forward rules on the router under "Firewall → Traffic Rules → Forwarding Rules" for configured protocols.

A rule for Forwarding traffic can be created as follows:

1. Navigate to "**Network Settings → LAN**" and create a **VLAN.**
2. Navigate to "**Wi-Fi Settings → SSIDs**" and create an **SSID** and assign to it the previously created **VLAN**.
3. Connect two devices (*ex: PC & phone*) to Grandstream router, first device to the default SSID (**default VLAN**) and the second device to the **SSID** created previously.



4. Navigate to "**Firewall → Traffic rules → Forwarding rules tab**" and create a new rule, select **ICMP protocol**, **ICMP Type** (any), Source Group (previously created **VLAN**), Destination Group (**Default VLAN**) and **Action = Accept**.



ICMP example

5. From the device connected to the default SSID (**default VLAN**) try pinging the other device on the other **VLAN** before applying the rule and after.

Before applying the Forwarding rule

```
C:\Users\Jawad>ping 192.168.7.146

Pinging 192.168.7.146 with 32 bytes of data:
Reply from 192.168.9.1: Destination port unreachable.
Reply from 192.168.9.1: Destination port unreachable.
Reply from 192.168.9.1: Destination port unreachable.
Reply from 192.168.9.1: Destination port unreachable.
```

After applying the Forwarding rule

```
C:\Users\Jawad>ping 192.168.7.146

Pinging 192.168.7.146 with 32 bytes of data:
Reply from 192.168.7.146: bytes=32 time=60ms TTL=63
Reply from 192.168.7.146: bytes=32 time=66ms TTL=63
Reply from 192.168.7.146: bytes=32 time=79ms TTL=63
Reply from 192.168.7.146: bytes=32 time=95ms TTL=63
```

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

TRAFFIC RULES TABLE

The following table provides an explanation of each field related to the traffic rules feature.

Field	Description
Name	Specify a name for the traffic rule.
Status	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 the dropdown list or All. Available Options: 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.
Action	Select which action to perform for the given traffic rule. Three options are available: Accept, Deny, or Drop.

SUPPORTED DEVICES

The following devices support the Firewall Traffic Rules features:

Model	Firmware
GWN700X	1.0.5.6 or newer
GWN7062/GWN7052(F)	1.0.9.10/1.0.9.9 or newer
GCC60xx	1.0.1.8 or newer