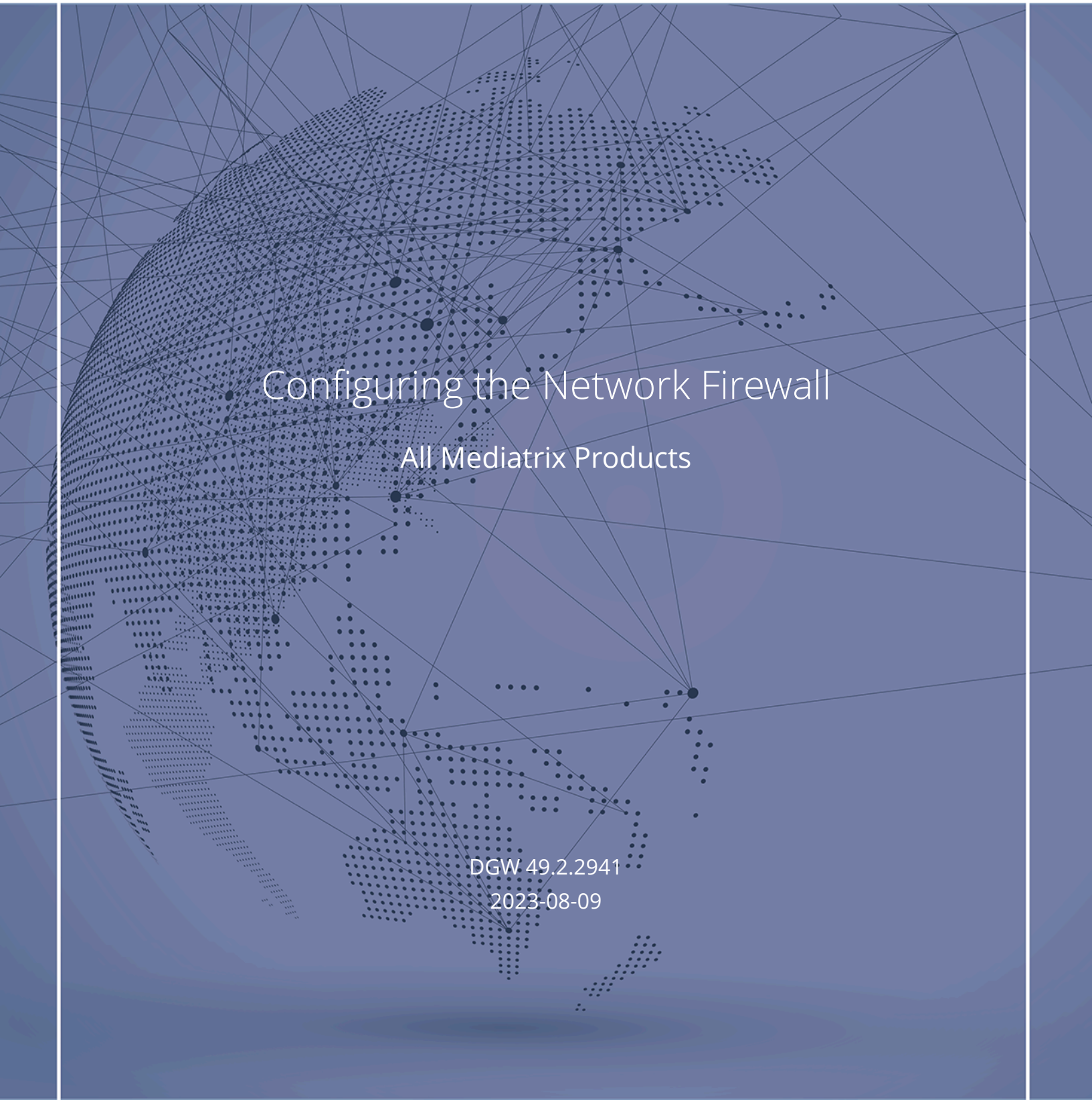

Configuring the Network Firewall

All Mediatrix Products

DGW 49.2.2941

2023-08-09

Table of Contents

Basic Concepts

Network Firewall

The Network firewall allows you to dynamically create and configure rules to filter incoming packets forwarded by the Mediatrix unit among its network interfaces, when the unit is used as a router. Its main functionality is to secure the traffic routed from and to the devices inside the local network.

Since this is a network firewall, rules only apply to incoming packets forwarded by the unit. The traffic is analyzed and filtered by all the rules configured. If no rule matches the incoming packet, the default policy is applied. A rule's priority is determined by its index in the table. Rules using Network Names are automatically updated as the associated IP addresses and network mask are modified. If the Network Firewall service is stopped, all forwarded traffic is accepted, this tab is greyed out and the parameters are not displayed.

Of course, the more rules are enabled, the more overall performance is affected. You can use a maximum of 20 rules.

Firewall Rule Order - Important

The order in which the incoming packets are tested against the rules is important if you want to make sure that they actually have a filtering effect on incoming packets.

Rules can be configured to accept or to decline packets. But, always put the most restrictive rules first as they are executed sequentially starting with the first one listed at the top of the table i.e. make sure that the order in which the rules are executed does not cause a rule to be systematically excluded.

For example:

- If the first rule excludes all packets coming from a specific net mask, providing a second rule for an IP address with that same net mask will have no effect.
- If the first rule indicates actions to be taken for a specific IP address with a given net mask, and the second rule indicates to exclude all IP addresses with that net mask, both rules will be applied and have a result on the incoming packets.

Basic Tasks

Configuring the Network Firewall

Steps

1) Go to **Network**/**Network Firewall**.
2) In the **Network Firewall Configuration** table, set the **Default Policy** to **Accept**.

   Note: Setting the Default Policy to "Accept" means that all forwarded traffic is accepted. for more details on network firewalls, refer to the DGW Configuration Guide - Configuring the Network Firewall published on the Media5 Documentation Portal.

3) Click **Save & Apply**.

Result

Disabling the Network Firewall

Before you start

You must have a Network Interface created.

Steps

1) Go to **Network**/**Network Firewall**.
2) In the **Network Firewall Configuration** table, set the **Default Policy** to **Accept**.
3) In the **Network Firewall Rules** table, from the **Activation** column, select **Disable** for all the rules.
4) Click **Save**.

   Caution: Take the time to carefully review your rules before continuing to the next step.

5) Click **Save & Apply** to apply all changes to the configuration.

Result

All incoming packets will be accepted.

Configuring Black Listing Duration

Steps

1) Go to **Network/Network Firewall**.
2) In the **Network Firewall Configuration** table, set the **Blacklist Timeout**
3) Set the **Blacklist Rate Limit Timeout**.
4) Click **Save**.

Caution: Take the time to carefully review your rules before continuing to the next step.

5) Click **Save & Apply** to apply all changes to the configuration.
6) Click **restart required services**, located at the top of the page.

Result

Blacklisting parameters will be updated. Remember that for blacklisting to be used, at least one rule must have blacklisting enabled.
If a rule with the **Black listing enable** box checked matches a packet and no **Rate Limit Value** was set, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration of the **Blacklist Timeout**.

If a rule with the **Black listing enable** box checked matches a packet and the **Rate Limit Value** has been reached, then the source address of the packet will be black listed and all packets coming from this address will be blocked for the duration set for the **Blacklist Rate Limit Timeout**.

Example

Firewall Port Opening Example

This generic example shows how to allow remote clients to communicate with the IP office located at the LAN side of the Mediatrix unit.

In this example:

- The default policy is **Drop**, meaning that any packet that does not match the network firewall rules configured in the **Network Firewall Configuration** table will be dropped.
- To use the network firewall, IPv4 Forwarding (under IP Routing" tab), must be enabled. Without the forwarding, the network firewall is irrelevant because no packet will get passed from Uplink to LAN.

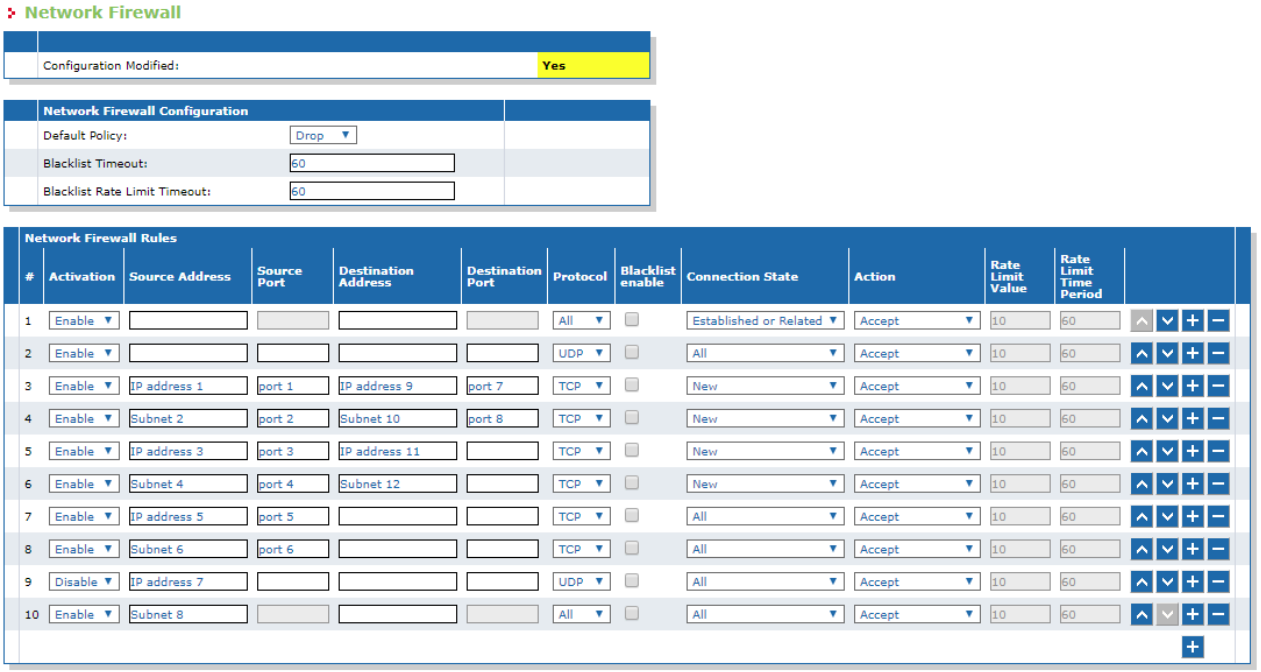

Table 1:

Rule	
1	All packets matching an existing connexion are accepted.
2	All packets coming through UDP are accepted.
3	New packets coming from the IP address 1 and port 1 with a destination to IP address 9 and port 7 through TCP, will be allowed.
4	New packets coming from Subnet 2 and port 2 with a destination to Subnet 10 and port 8 through TCP, will be allowed.
5	New packets coming from the IP address 3 and port 3 with a destination to IP address 11 with any port through TCP, will be allowed.
6	New packets coming from the Subnet 4 and port 4 with a destination to Subnet 12 with any port through TCP, will be allowed.
7	Any packet coming from IP address 5 and port 5 to any destination and port through TCP, will be allowed.
8	Any packet coming from Subnet 6 and port 6 to any destination and port through TCP, will be allowed.
9	This rule will not be applied as it is disabled.
10	Any packet coming from Subnet 8 and any port to any destination and port through TCP, will be allowed.
Default	Packets are dropped.

Online Help

If you are not familiar with the meaning of the fields and buttons, click **Show Help**, located at the upper right corner of the Web page. When activated, the fields and buttons that offer online help will change to green and if you hover over them, the description will bedisplayed.

DGW Documentation

Mediatrix devices are supplied with an exhaustive set of documentation.

Mediatrix user documentation is available on the Media5 Documentation Portal.

Several types of documents were created to clearly present the information you are looking for. Our documentation includes:

- **Release notes**: Generated at each GA release, this document includes the known and solved issues of the software. It also outlines the changes and the new features the release includes.
- **Configuration notes**: These documents are created to facilitate the configuration of a specific use case. They address a configuration aspect we consider that most users will need to perform. However, in some cases, a configuration note is created after receiving a question from a customer. They provide standard step-by-step procedures detailing the values of the parameters to use. They provide a means of validation and present some conceptual information. The configuration notes are specifically created to guide the user through an aspect of the configuration.
- **Technical bulletins**: These documents are created to facilitate the configuration of a specific technical action, such as performing a firmware upgrade.
- **Hardware installation guide**: They provide the detailed procedure on how to safely and adequately install the unit. It provides information on card installation, cable connections, and how to access for the first time the Management interface.
- **User guide**: The user guide explains how to customise to your needs the configuration of the unit. Although this document is task oriented, it provides conceptual information to help the user understand the purpose and impact of each task. The User Guide will provide information such as where and how TR-069 can be configured in the Management Interface, how to set firewalls, or how to use the CLI to configure parameters that are not available in the Management Interface.
- **Reference guide**: This exhaustive document has been created for advanced users. It includes a description of all the parameters used by all the services of the Mediatrix units. You will find, for example, scripts to configure a specific parameter, notification messages sent by a service, or an action description used to create Rulesets. This document includes reference information such as a dictionary, and it does not include any step-by-step procedures.

Copyright Notice

Copyright © 2023 Media5 Corporation.

This document contains information that is proprietary to Media5 Corporation.

Media5 Corporation reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by Media5 Corporation.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.

media5 corporation

media5corp.com