

Configuring Local Firewalls

All Mediatrix Products

DGW 49.2.2941

2023-08-09

Table of Contents

Basic Concepts	3
Local Firewall	3
Firewall Rule Order - Important	3
Basic Tasks	4
Configuring the Local Firewall	4
Disabling the Local Firewall	5
Configuring Black Listing Duration	5
Setting the No Match Local Firewall Default Policy	6
Examples	7
Generic Whitelist	7
Whitelist for Internet Hacker Protection	8
Generic Blacklist	9
Online Help	11
DGW Documentation	12
Copyright Notice	13

Basic Concepts

Local Firewall

The local firewall allows you to create and configure rules to filter incoming packets that have the Mediatrix unit as destination.

The Local Firewall is therefore a security feature that allows you to protect your Mediatrix unit from receiving packets from unwanted or unauthorized peers. As a best practice, the way the Local Firewall should work is to, by default, drop all incoming packets (i.e. not forward the packet to its destination) and let incoming packets go through only if they match a rule requirements. However, incoming packets for an IP communication established by the Mediatrix unit are always accepted (Example : If the Mediatrix unit sends a DNS request, the answer will be accepted).

When configuring the Local Firewall, enabling the default policy to drop all incoming packets should be the last step you perform otherwise, you may lose contact with the Mediatrix unit, even if you are performing the initial configuration of your system. Therefore, start by creating the rules that allow the Mediatrix unit to accept some packets. This way communication will not be lost and you will not need to perform a partial or factory reset to reconnect with the Mediatrix unit.

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

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 Local Firewall

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Rules** table, complete the fields as required.
- 3) In the **Local Firewall Configuration** table, from the **Default Policy** selection list, select **Drop**.

IMPORTANT: Before setting the **Default Policy** to **Drop**, i.e. to apply the local firewall rules and to drop any incoming call that does not match a rule, review your rules to make sure that at least one rule accepts incoming packets for management, otherwise the communication with the Mediatrix Sentinel will be lost.

Note: For example, if the Web interface is used for management (HTTP port 80) via the unit's LAN interface (default IP address = 192.168.0.10), then the following rule could be added: **Activation=Enable / Destination Address=192.168.0.10 / Destination port=80 / Protocol=TCP / Action=Accept**

Note: For blacklisting to be used, at least one firewall rule must have the **Black listing enable** box checked.

Note: Before setting the **Default Policy** to **Drop**, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mediatrix Sentinel will be lost.

- 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

The Local Firewall will drop packets without any notification message.

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**.

Disabling the Local Firewall

Before you start

You must have a Network Interface created.

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local Firewall Configuration** table, set the **Default Policy** to **Accept**.
- 3) In the **Local 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.
- 6) Click **restart required services**, located at the top of the page.

Result

All incoming packets will be accepted.

Configuring Black Listing Duration

Steps

- 1) Go to **Network/Local Firewall**.
- 2) In the **Local 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**.

Setting the No Match Local Firewall Default Policy

Steps

- 1) Go to **Network/Local Firewall**.

Note: Before setting the **Default Policy** to **Drop**, i.e. to apply the local firewall rules and to drop any incoming call that does not match a rule, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mediatrix Sentinel will be lost.

- 2) In the **Local Firewall Configuration** table, set the **Default Policy** to **Drop**.

Result

The local firewall rules will be applied and if an incoming call does not match a call it will be dropped.

Examples

Generic Whitelist

All incoming calls are dropped unless they match one of the firewall rules which are acting on the incoming packets going towards the Mediatrix gateway.

Local Firewall

Configuration Modified:	Yes
-------------------------	-----

Local Firewall Configuration	
Default Policy:	Drop
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules											
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable	Lan1/		Lan1		All	☐	Accept	10	60	^ v + -
2	Enable	Uplink/		Uplink		All	☐	Accept	10	60	^ v + -
3	Enable	IP address		Uplink	80	TCP	☐	Accept	10	60	^ v + -
4	Enable	IP address		Uplink	443	TCP	☐	Rate limit source	10	60	^ v + -
5	Enable	Subnet		Uplink	22	UDP	☐	Accept	10	60	^ v + -
6	Enable	Subnet		Uplink	5060	UDP	☐	Accept	10	60	^ v + -
7	Enable	Subnet		Uplink	5004-6020	UDP	☐	Accept			^ v + -
											+

Result:

Rule #	
1	Any incoming packet from the LAN subnet having the unit's LAN host IP address as a destination is allowed.
2	Any incoming packet from the Uplink subnet is allowed (assuming this is a private network).
3	Any HTTP incoming packet from the selected IP address having the unit's Uplink IP address as a destination through TCP port 80 is allowed.
4	Any HTTPS incoming packets from the selected IP address having the unit's Uplink IP address as a destination through TCP port 443 is allowed, but rate limited to 10 new connection attempts per 60 sec.
5	Any SSH incoming packets from the selected subnet having the unit's Uplink IP address as a destination through TCP port 22 is allowed.
6	Any SIP incoming packets from the selected subnet having the unit's Uplink IP address as a destination through UDP port 5060 is allowed.
7	Any RTP and T.38 incoming packet from the selected subnet having the unit's Uplink IP address as a destination through UDP port range 5004-6020 is allowed.
Default	All other incoming packets are rejected.

Whitelist for Internet Hacker Protection

Simple Local Firewall rules to protect the unit from Internet hackers. All incoming calls are dropped unless they match one of the local firewall rules which are acting on the incoming traffic towards the Mediatrix gateway.

Local Firewall

Configuration Modified:	Yes
-------------------------	-----

Local Firewall Configuration	
Default Policy:	Drop
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period		
1	Enable	Lan1/		Lan1		All	☐	Accept	10	60	▲▼+ -	
2	Enable	Uplink/		Uplink		All	☐	Accept	10	60	▲▼+ -	
3	Enable	IP address		Uplink		All	☐	Accept	10	60	▲▼+ -	
4	Enable	Subnet		Uplink		All	☐	Accept			▲▼+ -	
												+

Result:

Rule #	Description
1	Any incoming packet from the LAN subnet is allowed.
2	Any incoming packet from the Uplink subnet is allowed (assuming this is a private network).
3	Any incoming packet from selected IP address is allowed (e.g. this is the management server).
4	Any incoming packet from the selected subnet is allowed (e.g. this is the Core SIP server, SBC and its media gateways).
Default	Any incoming packet not meeting the criteria of these rules is dropped.

Generic Blacklist

The default policy is set to "Accept" but the firewall rules are Blacklists acting on incoming traffic towards the Mediatrix gateway:

Local Firewall

Configuration Modified:	Yes
-------------------------	-----

Local Firewall Configuration	
Default Policy:	Accept
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

Local Firewall Rules												
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period		
1	Enable			Uplink	22	TCP	☐	Drop	10	60	▲▼	+ -
2	Enable	Subnet				All	☐	Drop	10	60	▲▼	+ -
3	Enable	IP address		Uplink	80	TCP	☐	Drop	10	60	▲▼	+ -
4	Enable	Subnet		Lan1		All	☐	Reject	10	60	▲▼	+ -
5	Enable	IP address		Lan1	5060	UDP	☐	Rate limit source	10	60	▲▼	+ -
												+

Subnet example: 192.168.1.0/24

Result:

Rule #	Description
1	Any incoming packet going to the Uplink interface through TCP port 22 (SSH) is dropped.
2	Any incoming packet coming from the specified subnet is dropped.
3	Any HTTP incoming packet coming from the specified IP address to the Uplink interface through TCP port 80 is dropped.
4	Any incoming packet from the specified subnet to the Lan1 interface is rejected, and an ICMP message is returned.
5	Any SIP incoming packets from the specified IP address to the Lan1 interface through UDP port 5060 is rate limited to 10 new connection attempts per 60 sec.
Default	All other incoming packets are accepted.

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 be displayed.

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.



media5corp.com