



mailcleaner

A P P L I A N C E

F O R M A T I O N

F O R R E S E L L E R S



© 2009 Fastnet SA, St-Sulpice, Switzerland. All rights reserved.

Reproduction in whole or in part in any form of this manual without written permission of Fastnet SA is prohibited.

MailCleaner is a registered trademark of Fastnet SA.

All other trade names and trademarks cited in this manual are the properties of their respective owners.

www.mailcleaner.com

1	The Appliance	4
	"MailCleaner Security Gateway" or MailCleaner MC200	4
	Options	4
2	Infrastructure planning	5
	Network environment.....	5
	Network connectivity.....	5
	Typical MailCleaner Installation	7
	Typical MailCleaner Installation with Firewall and DMZ.....	7
3	Registration	8
	Getting automatic updates.....	8
	<i>What is your reseller ID</i>	8
	<i>What is your reseller password</i>	8
	<i>What is this client ID</i>	8
	Finishing registration.....	9
4	Post installation	10
	Test A 10	
	Test B 10	
	Final step	10
5	Important note	11
	Firewall	11
	Call out	11
	Unique session by server	11
	White List / Warn List.....	11
	Bypass of MailCleaner	12
6	Diagnostics	13
	Verification of the headers	13

1 The Appliance

“MailCleaner Security Gateway” or MailCleaner MC200



Basic Unit: Intel Core 2 Duo 3 GHz processor, 2 GB of RAM and a 250 GB hard drive,

Options

- RAID with 2 * 250 GB: CHF 150
- 2 GB extra RAM: CHF 60
- "Premium" Support: pricing available by request

2 Infrastructure planning

Network environment

Please have on hand an IP address and a hostname to be dedicated to your MailCleaner. The hostname must be resolvable via DNS. MailCleaner also needs Internet access on a number ports. Make sure the firewall allows the following traffic:

From the Internet to MailCleaner:

- 25 TCP (SMTP, from ANY or potentially from a specific gateway).
- 80 and 443 TCP (HTTP(S), optional but required for user and administrative interfaces).

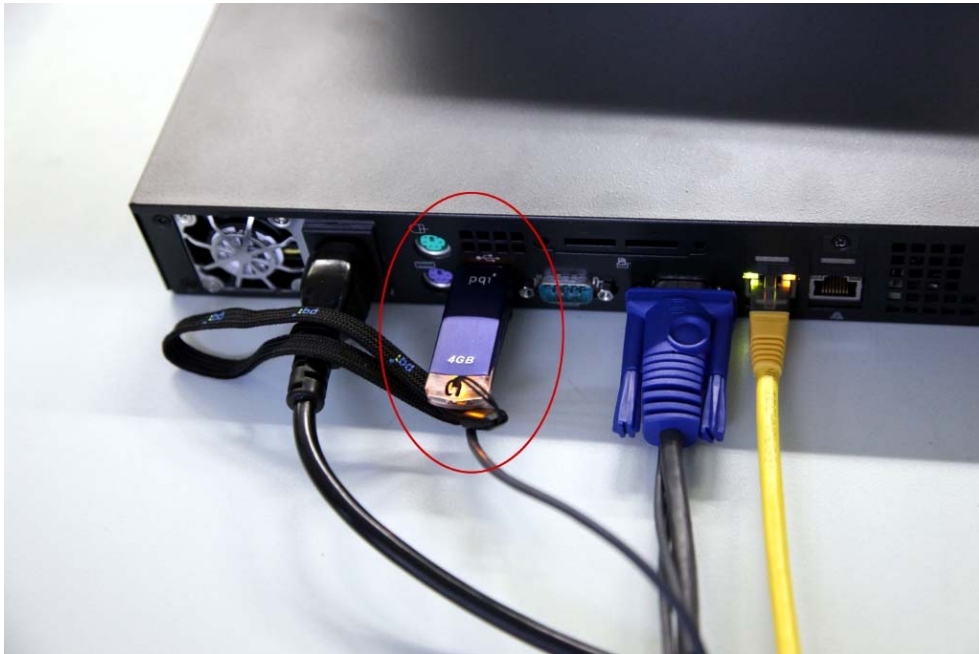
If your MailCleaner is in a private subnet behind a firewall, please do not forget to configure the necessary NAT rules to forward traffic from the WAN to your MailCleaner server.

From MailCleaner to the Internet:

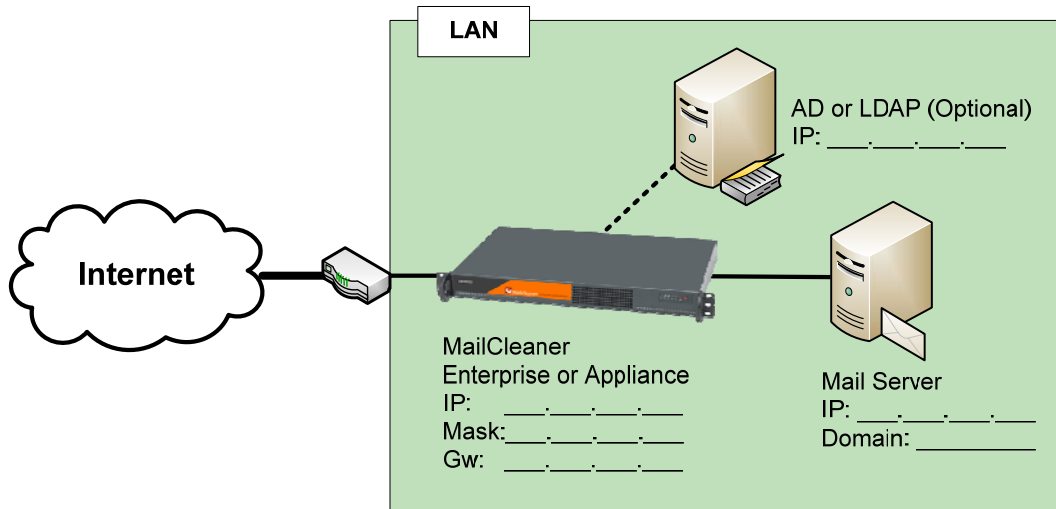
- 25 TCP (SMTP, to ANY or to a specific smtp gateway).
- 22 TCP (SSH, Mailcleaner updates, limited to 195.176.194.0/24 and 193.246.63.0/24).
- 80 and 443 TCP (HTTP(S), to ANY or to a specific gateway).
- 7 and 2703 TCP (Razor, to ANY).
- 24441 UDP (Pyzor, to ANY).
- 6277 UDP (DCC, to ANY).

Network connectivity

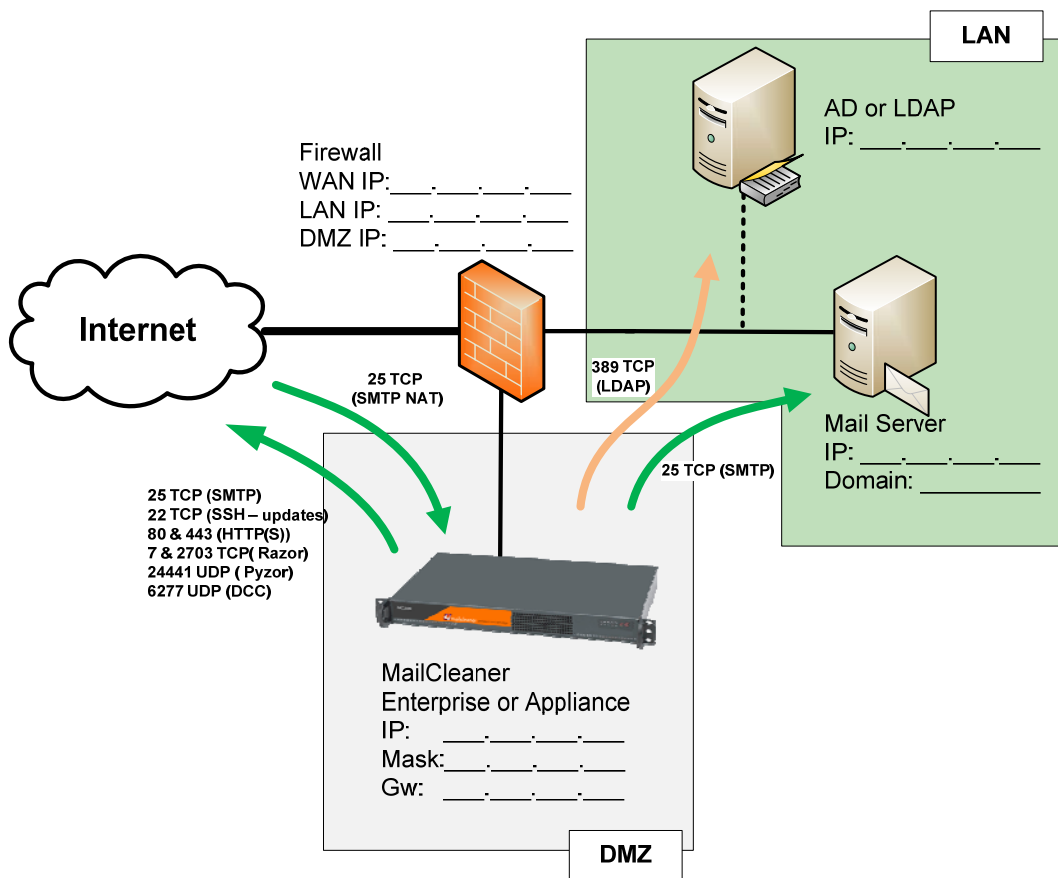
Use only the network connector located next to the power supply plugin on the back side of the appliance



Typical MailCleaner Installation



Typical MailCleaner Installation with Firewall and DMZ



!! For Premium support -> 22 TCP incoming from MailCleaner IPs

3 Registration

This step will allow your MailCleaner to access the automatic update center to receive operating system updates, patches and especially filtering rule updates.

Getting automatic updates

If you wish to get automatic updates for your MailCleaner, you may want to register with MailCleaner's update service. Once you get the settings back from our service (client id, reseller id/password, etc.), you must log on to the web admin interface, using the password provided during the installation, and go to:

Configuration -> Base system -> Registration

You must then answer some questions.

What is your reseller ID

The reseller ID as assigned by Fastnet SA; use 0 for an installation without updates.

What is your reseller password

The password associated with the reseller ID (leave empty for an installation without updates).

What is this client ID

The client (or customer) ID as assigned by Fastnet SA; use 0 for an installation without updates.

Click: "Register"

Note: Serial Number on the "MailCleaner License Certificate" is composed like:
reseller ID - client ID



Customer : End user Firma
Hauptstrasse 1
CH-8000 Zürich
Switzerland

MailCleaner License Certificate

Type : 1 year license

Content : Security Gateway Appliance

Description : Updates, basic support and feedback

Serial number : 6XXX-6YYY

Number of users : < 100

Period of license : From 01/12/2009 to 30/11/2010

Value Added Reseller : VAR AG
CH-3000 Bern

Distributor : Studerus AG
CH-8603 Schwerzenbach

MailCleaner is a registered Trademark of
Fastnet SA - Rue des Jordils 40 - 1025 St-Sulpice - Switzerland

www.mailcleaner.net

Finishing registration

When finished, this step will register your MailCleaner installation with our update service.

Available updates will then be fetched every 15 minutes.

Anti-virus definitions are updated every hour by default.

4 Post installation

You're almost finished! Now that you have completed the installation and registration of your MailCleaner, it is time to configure it for the domains that you wish to filter. Please connect your web browser to the MailCleaner web administrative console:

<https://yourmailcleanerhost/admin>

Go to "Configuration" -> "Domains"

Please configure the domains that you would like to protect.

Remember: MailCleaner will not be operational until it is configured for the domain(s) that you would like to filter.

Once you have completed your domain configuration you can now test your new installation.

Test A

Please verify that users of each domain can access the user web interface:

<https://yourmailcleanerhost/>

Test B

Verify that messages go correctly through your MailCleaner by directly sending a message for an existing user through your MailCleaner. For example, temporarily change your SMTP server in your mail software to point to your MailCleaner server, or initiate a manual SMTP session from a command console using the command `telnet yourmailcleanerhost 25`.

Final step

Once you have completed these two verifications, your MailCleaner installation is ready to be put in production. The final step is making your installation visible to the rest of the world.

Modify your email routing by changing the MX records for the filtered domains, or by altering your firewall or mail gateway configuration.

Note: Never use one MX for your MailCleaner and a secondary MX with higher priority directly to your mail server. Spammer now that and will bypass your MailCleaner.

Congratulations! Your installation is now complete.

5 Important note

Firewall

Be sure to respect the Firewall configuration required (open ports for DNS, updates,...)

See chapter 2 before "Infrastructure planning"

Call out

The call_out validation is very important.

For Exchange Servers please refer to our specific documentation:

http://www.mailcleaner.net/downloads/MailCleaner_Exchange07-03_config.pdf

Unique session by server

Some mail servers (including Exchange) are configured to accept only a maximum of connections per server.

If you add MailCleaner (or any gateway) between Internet and the mail server, this mail server could reject mail coming from MailCleaner for this reason.

Be careful of that point and adjust if necessary this limit on the final mail server

White List / Warn List

White listing is potentially very dangerous, please be careful with the use of white lists:

<http://www.mailcleaner.net/antispam/documentations/whitelist.html>

Warn listing is a more secure alternative to the white listing.

The warn list contains trusted sender addresses for which you want to be notified by mail whenever a message happens to be detected as spam. You can then immediately release the message in case of a filtering error.

Warning: this functionality should be used as a temporary solution as it decreases the overall protection.

To use WhiteList / Warn List you need to activate it in:

Configuration -> Anti-Spam -> Global settings

And you need to activate it for each domain that needs to use white/warn list

Configuration -> Domains -> filtering

Bypass of MailCleaner

Be careful to not activate a secondary MX directly to your mail server because spammer know that and will send spam directly to the final mail sever without going through MailCleaner.

On the final mail server you can also block smtp session that are not coming from MailCleaner or from the local network.

6 Diagnostics

Verification of the headers

In the quarantine, click on the middle button

