mailcleaner

ADMINISTRATOR FAQ

V 1.0

www.mailcleaner.net

1 Introduction 4

2 Infrastructure planning 5

Network environment 5
Typical MailCleaner Installation 6
Typical MailCleaner Installation with Firewall and DMZ 6
Network configuration 7
Configuring a domain 8

3 MailCleaner Configuration FAQ 9

General settings: defaults 9
General settings: company 10
Domains: general 10
Domains: delivery 10
Domains: address verification 11
Domains: authentication 11
SMTP: SMTP checks 12
SMTP: resources control 13
SMTP: TLS/SSL 14
SMTP: greylisting 14
Anti-Spam: global settings 14
Anti-Spam: TrustedSources 15
Anti-Spam: NiceBayes 16
Content protection: Global settings 16
Services: Web interfaces 17
Services: Database 17
Services: API 17

1 Introduction

Welcome to a world where the e-mail you get is the e-mail you want.

Thank you for your interest in the MailCleaner Security Gateway. This document will provide you through Frequently Asked Questions, the efficient way of securing your e-mail infrastructure within minutes. All information's refer to the MailCleaner Administration interface.

MailCleaner is an antivirus and anti-spam system that is extremely powerful and easy to setup. Based on the latest generation of filtering technologies, MailCleaner acts at the highest technical level of the network infrastructure of your company, organization or ISP.

Placed before your mail server in the messaging path, MailCleaner will protect your mailboxes from any potentially dangerous and unwanted content and prevent useless messages from reaching your internal network.

MailCleaner Security Gateway is designed to handle large-scale attacks. Its balance of simplicity and robustness makes it a perfect fit as the main network entry point for your messaging system.

2 Infrastructure planning

MailCleaner in your network

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 of ports. Make sure the firewall allows the following traffic:

From the Internet to MailCleaner:

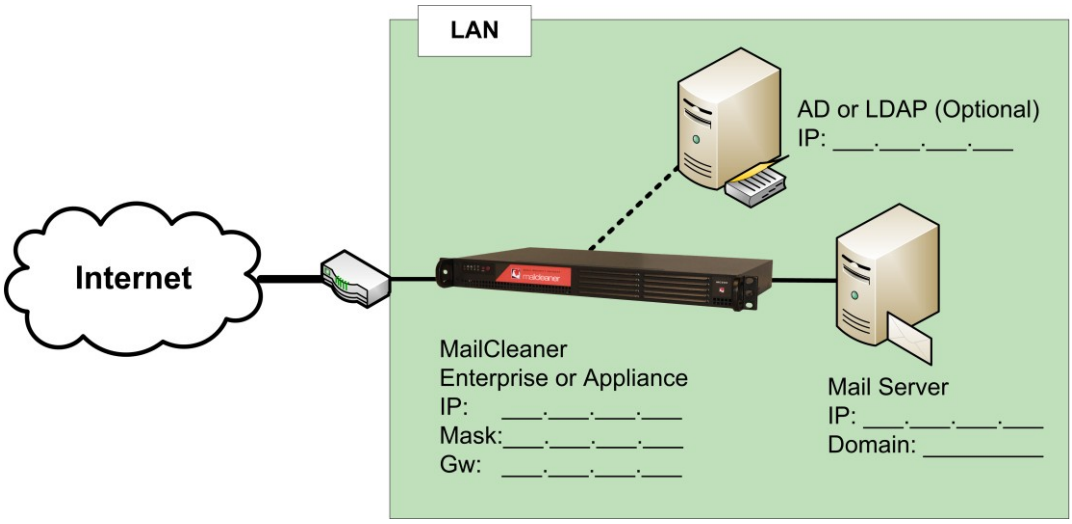
- *25 TCP (SMTP, from ANY or potentially from a specific gateway).*
- *80 and 443 TCP (HTTP(S), optional but required for user and administrative interfaces).*

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.

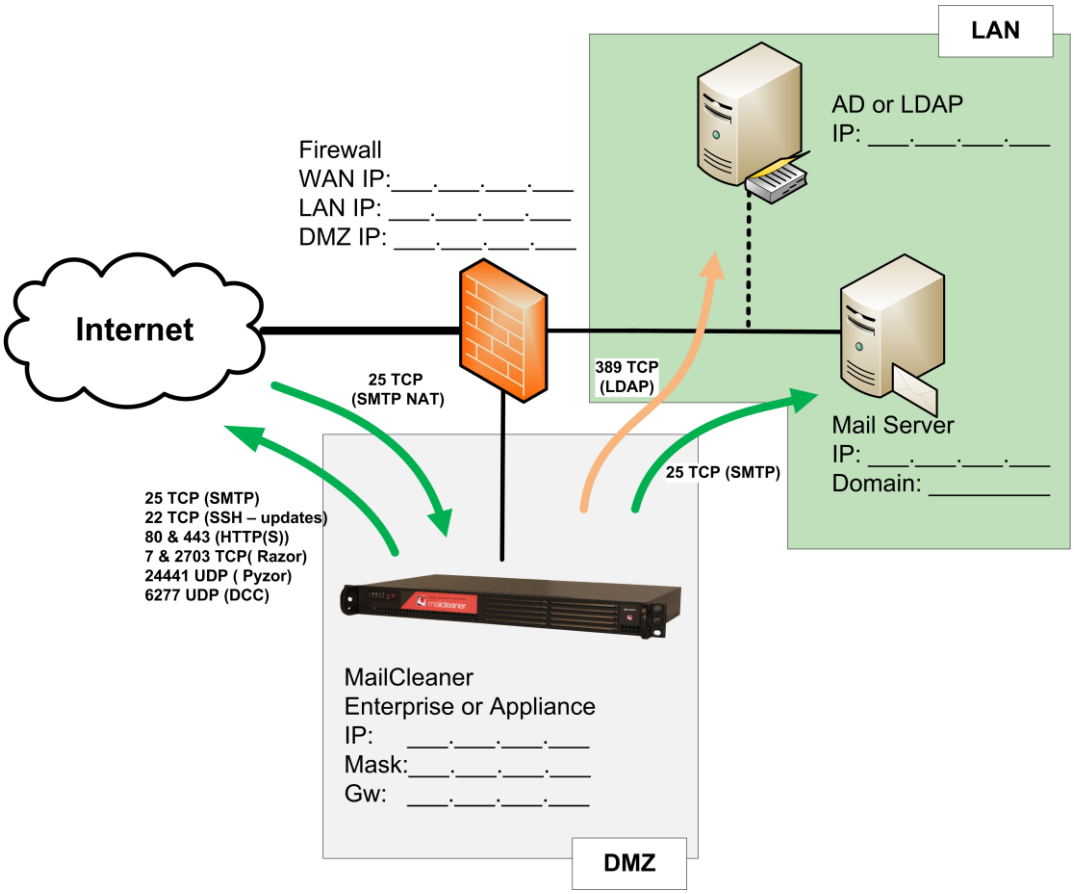
From MailCleaner to the Internet:

- *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).*

Typical MailCleaner Installation



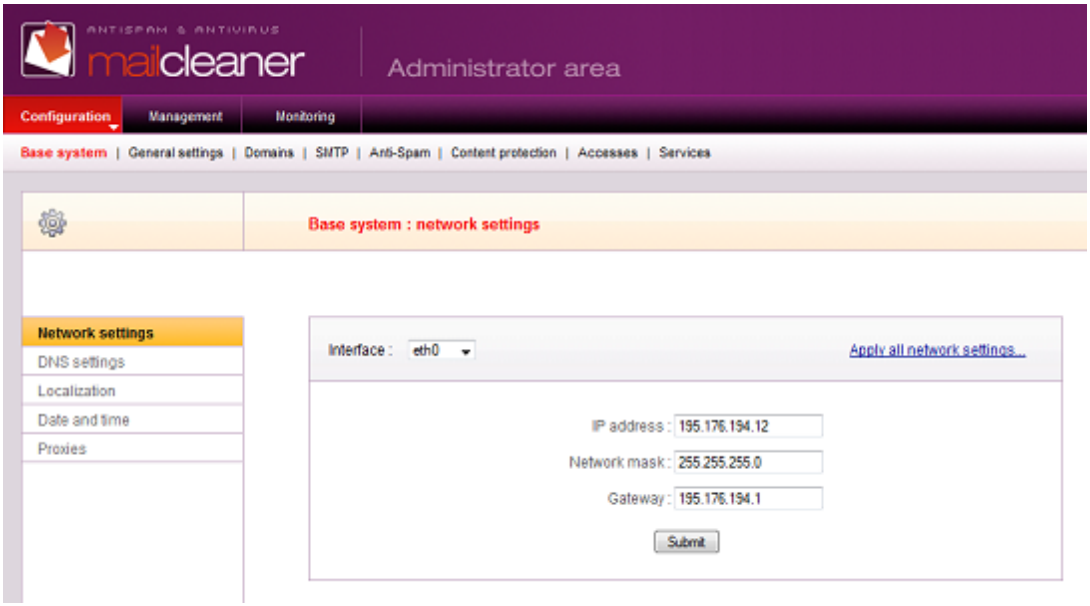
Typical MailCleaner Installation with Firewall and DMZ



Network configuration

From the main administration menu, click on the “Base system” entry, under the “Configuration” section, as shown in figure 5-2.

Figure 5-2 *Network configuration menu entry*



On figure 5-3, you will see the network configuration panel. Enter the different parameters that match your network topology and then click on “Submit” button to activate your changes. You can optionally configure the second physical network interface available on the unit as well..

Important: You may be disconnected after applying network changes. If so, reconnect your browser to the new IP address in order to return to the MailCleaner administration web-based interface.

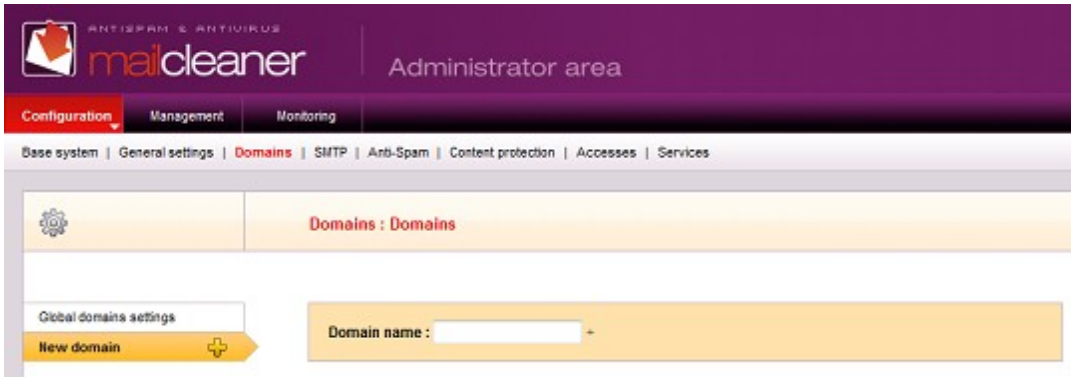
Figure 5-3 *Network configuration panel*

Configuring a domain

The second important step before your MailCleaner can start filtering mail is to provide the list of mail domains it will be accepting, filtering and the relaying mail for.

Click on the “Configuration” entry under the domain section in the main navigation menu, as shown in figure 5-4.

Figure 5-4 *Domain configuration menu entry with “New domain”*



Click on the “New domain” link to open the new domain panel on the right. Two values are required: the domain name and the destination server(s).

3 MailCleaner Configuration FAQ

This section will guide you into the configuration menus of your system, through common and typical questions.

General settings: defaults

Questions:

False negative / positive reporting address
- We assume that these need to be our email addresses?
- How are these used?
- If someone sends a message to one of these addresses how do we take action on it?

These are addresses where users can send filtering errors that MailCleaner can potentially do.

False negatives are real spam that wasn't correctly detected as spam.

False positives are valid messages that were incorrectly detected as spam by MailCleaner.

These mistakes can be forwarded to these addresses for further analysis and filter correction by our services.

You can either put your own addresses here, so that you can have a look and some checks on what is actually sent to our analysis center (in case of privacy concerns for example), or you can directly setup our analysis center addresses if you don't want any control on this.

Our analysis center addresses are:

spam@mailcleaner.net for false negatives

nospam@mailcleaner.net for false positives

If you choose to use your own addresses, make sure to forward us the valid requests so that we can actually adapt the filtering or provide help to avoid further mistakes.

You can find more information on this in the MailCleaner User Manual, available in the help section of the Web User Interface.

General settings: company

Questions:

How is the contact email address used?

These information's are purely informative and can be left empty.

They are aimed at providing information on the people to contact or who are responsible for the system. i.e. in case the sysadmin has change.

Domains: general

Questions:

- The top three options (System mail sender address, false negative reporting address, false positive reporting address) are all set in General Settings: defaults. Do these need to be entered again?
- The last two options are set in General Settings: company. Do these need to be set again?

No, if you leave these empty, the default configured in the General settings will be used.

You can however fill them with specific addresses, if you want only one domain to be monitored for privacy measures.

Domains: delivery

Questions:

- Use MX resolution. What does this do?

The MX resolution option means that MailCleaner, instead of delivering to the host defined in the destination server, will do a MX resolution to find out where to deliver mail.

This option can be useful in case you have some address rewriting in front of the MailCleaner in order to have a dynamic destination server resolution.

This is however a quite rare case and should not be used in other cases because it can lead to delivery loops (as the MX record is likely to be the MailCleaner itself).

Domains: address verification

Questions:

- Callout connectors. What is a “Callout connector” and what does it do?

The callout is a functionality that allows MailCleaner to **dynamically validate the existence of the destination address**.

When a new connection happens to the MailCleaner, the sending server provides MailCleaner with the sender address and the recipient address (your user). At this moment, and before accepting the remaining part of the message, MailCleaner will do a call to your destination server (or to the callout server if different) to ask if this destination address exists or not.

If the destination server accepts the address, then MailCleaner will accept the message. If it refuses it (with a 550 user unknown error for example), MailCleaner will refuse the message.

This is really handy in order to avoid dictionary attacks and useless filtering of invalid users.

MailCleaner can currently do this call with two different protocols.

The SMTP callout **is the most efficient** one as it is fast and very stable. All it does is effectively "mimic" the SMTP dialog MailCleaner receives, to the destination server. If it gets a 550 error code, then the message is refused. Otherwise the message is accepted and processed. The only requirement is that the destination server must refuse invalid recipient during the SMTP dialog. Almost all mail servers do that by default, but some still don't. Exchange is the main example of that. Fortunately, it is quite easy to enable this behavior. You should check the following document if you need to do so: http://www.mailcleaner.net/downloads/MailCleaner_Exchange07-03_config.pdf

The LDAP/AD connector will do a LDAP call to the callout server. This is a heavier protocol and thus is only advise of there is no other solution. Also, it is a bit more difficult to configure.

Domains: authentication

Questions:

- What are the benefits of using POP3 vs IMAP vs SMTP vs Local authentication?
- What is Local authentication and how is it used?
- User name modifier. Is this applicable to a MailCleaner server?
- How can Address Lookup be used best in a situation with 100 different domains?

The POP3, IMAP and SMTP authentication connectors are remote. This means that the credentials are note stored on the MailCleaner, but on the authentication server (usually your mail server).

MailCleaner will then forward the authentication to this server allowing users to use the same login information as for their mail (or desktop). This also has the advantage of being completely dynamic, which means that you don't need to create/update/delete accounts on the MailCleaner. Once a new account has been created on the authentication server (or mail server), it will be immediately available on MailCleaner.

The difference between POP3, IMAP and SMTP is purely convenient for you. It does not make any difference for MailCleaner, but one or the other might be preferable for you (for policy reasons for example).

The Ldap/Active Directory connector is also a remote connector but the other advantage of being exhaustive and being able to provide information on the account. This means that MailCleaner will also be able to fetch all addresses and aliases that are linked to a user.

The local authentication is advised only for cases where it's absolutely not possible to reach any authentication or mail server, which is a very rare case. It is not advised, otherwise it imposes administrators to manage accounts manually, instead of being dynamic like for the other remote connectors.

The username modifier is used by MailCleaner to define the format of the username that is actually sent to the authentication server. Some servers only accepts username with domains (i.e. username@domain) while other only accepts the username (username). This totally depends on the authentication server.

As MailCleaner is a full multi-domain solution, and allows each domain to have it's own authentication settings, it has to know for which domain a user is attempting to log in. That way, the user will always need to log in using the username@domain on the MailCleaner. But in the case the authentication server only needs the username, then using the "username only" setting for the domain authentication, will tell MailCleaner to use the correct syntax.

The address lookup is used by MailCleaner to either fetch (for exhaustive connectors, like Ldap), or build the addresses that will be added to the user account. For example, in an Active Directory, if a user has many different SMTP addresses, MailCleaner will be able to fetch them using the "fetch addresses from ldap directory" and display the correct quarantines to the user. If this information is not available, then MailCleaner can "build" it by adding the domain to the username (which is generally the case).

Please note that this does not have any impact on the filtering, as all addresses accepted by the destination server will still be filtered. But this is only used for the MailCleaner Web User Interface and to correctly display the addresses to the user. Of course, the user can still add/remove/edit the addresses that he needs to see in his quarantine.

Concerning the multi-domain, MailCleaner has being built on that purpose. So it is possible to either define a default value for all domains that are being added, or either specify a different authentication scheme for each one (if you have many external domains for which you are only doing the filtering for example).

SMTP: SMTP checks

Questions:

We assume that this only applies to mail that is sent using the MailCleaner server as the SMTP server i.e. my email client uses mailcleaner.domain.net as its SMTP address?

- Is there a way of turning SMTP off so that hosts cannot connect directly to the MailCleaner server to send email?

Originally, and by default, MailCleaner is only an Incoming gateway. Which means it is only aimed at receiving external mail for your domains and to deliver them to your mail server.

Now, MailCleaner has many features that allow MailCleaner to be also used as an **outgoing gateway**. There are two ways to allow that:

- setting allowed IP addresses in the "Configuration -> Connection control -> 'Allow external relaying for these hosts' " field

- enabling the "Allow users to use SMTP authentication" in the authentication subpanel of each domain configuration.

If none of the above are set, then MailCleaner will never allow messages being relayed to the outside. Only messages for the domains configured will ever be accepted.

If this feature is required, then users are advised to use port 587, which is the standard for mail submission. MailCleaner will not apply any RBL check on this port but will only accept messages allowed to relay (either by a specifically allowed IP address, of by users using SMTP if it has been enabled).

The settings in the SMTP checks panel are applied for all incoming connections, and only the two last options (Scan relayed and Mask IP address) are for the relayed messages.

By default, SMTP relaying is not permitted on the MailCleaner.

SMTP: resources control

Questions:

- What does “enable per trusted host rate limit” do? Is this configurable?

All these settings applied to the incoming connection to MailCleaner. This means all messages being sent to your domains.

Some hosts might be defined as "trusted", for example if you have some gateway (MX) in front of MailCleaner.

The default settings usually are quite good for almost any situation (from low to high load).

The rate limiting allows you to restrict the number of connections allowed for a period of time. This can be useful to protect against DoS attacks.

These restrictions applied by default to every host connecting to the MailCleaner, but you can setup other (usually less strict) restrictions to the hosts that are defined as "trusted" (either from "Configuration -> Connection control -> 'Allow external relaying for these hosts' ", or from "Configuration -> Anti-spam -> Global Settings -> 'Trusted IPs/Networks' ").

As soon as you check the "Enable per host rate limit" or "Enable per trusted host rate limit" option, the settings will appear.

SMTP: TLS/SSL

Questions:

- What is this?

This panel allows you to setup a SSL certificate in order to have the SMTP service of MailCleaner be able to encrypt connections on both incoming and outgoing path.

Click on the "Enable SSL/TLS" checkbox to see more configuration options.

SMTP: greylisting

Questions:

“Avoid greylisting for these domains”.
This appears to be similar to Global domains settings -> filtering -> enable greylisting.
Which screen takes precedence?

- We would like to be able to switch off greylisting if we can.

This "Avoid greylisting for these domains" option is only for the incoming message. This allows avoiding doing greylisting on certain domains that do not interact correctly with this technique, such as gmail, hotmail and so...

By default the greylisting is off, but can be turned "On" on a per domain basis, through the filtering subpanel of the domain configuration.

By the way, this technique is not really clean and thus should be avoided whenever possible (this is why it is disabled by default).

Generally, the "Configuration -> Domains -> Global domains settings" is the way you can configure the default values for domains that are being added to the system. However, once a domain is created, it has its own setup and then is independent of this configuration panel.

Anti-Spam: global settings

Questions:

If we enter a trusted IP or network in this box does this mean that those IP address(es) will not go through the Anti-spam system?

- What is the correct notation for a network in this box e.g. 192.168.1.1/27 or 192.168.1.1 255.255.255.224

- What do the “enable access to whitelists” and “enable access to warnlists” tick boxes do?

No, messages sent by the IP addresses in the "Trusted IPs/networks" box will still be scanned. However, MailCleaner will forget the last Received header (the one from this host), and apply all anti-spam check the previous host. This is useful is you have a SMTP gateway in front of MailCleaner which is receiving the messages from the internet and then forwarding them to MailCleaner. That way, MailCleaner will be able to play the anti-spam check in the real external host, and not your internal, trusted system.

Of course, if there is no other Received header, meaning that the message was originally issued from the trusted host, then the message will be fully trusted.

The syntax is standard CIDR notation, such as 192.168.1.0/24, one IP or network by line.

The whitelist and warnlist flag enable the whole white/warn listing in MailCleaner. Without this check enabled, nobody will be able to access and manage the white/warn lists.

If enabled, the whitelists must also be enabled in the domain configuration (subpanel filtering) to be effectively active.

We placed these protections because whitelisting is a very dangerous feature. Although it seems something quite common and natural, it is really badly used and thus very dangerous.

The fact is that the whitelist is based on information (sender address) that is trivial to forge and fake. This makes it very easy for a spammer to circumvent any filtering by correctly forging the sender address of their spam (which is more and more often the case).

This is why **we strongly recommend users not to use whitelists**.

The warnlist is a mitigation of this risk. The principle here is the same as for the whitelist, but instead of letting the message go through (leading the user to believe the filter didn't detect the spam), it will put the message in quarantine and warn the recipient user that a message from this sender has been blocked. Then through a simple link, the user will be able to release and receive the message.

Although this is not the ultimate solution, it will help much when a spammer abuses someone's address book in order to bypass all filtering.

Anti-Spam: TrustedSources

Questions:

- What does Enable all trusted path detection mean?
- What is the effect of entering something into Known good authenticated SMTP servers box?
- Should this be a FQDN or an IP address?
- What does Authenticated SMTP servers search string mean?
- What is the format of the data entered here?

The "all trusted path detection" is the way MailCleaner detects that a message is all internal and was not issued by an external host. This generally means that the message can be fully trusted and thus will avoid anti-spam checks. This is a good way to ensure that no internal message will ever be blocked by MailCleaner.

On top of that, MailCleaner also has the capacity to detect if a message has been sent through a known and trusted authenticated SMTP server. This may be the case if you have some mobile users which use one of your server to send messages through an authenticated SMTP session. This will also help MailCleaner detect that these are good messages.

You should put IP addresses here.

The "search string" is any string that is present in the header added by the authentication server and which is pretty unique to it. This will help to enforce the check, but is not strictly required.

Anti-Spam: NiceBayes

Questions:

"Maximum message size". What happens if a message is greater than this size? Is it still filtered? Is it blocked? What happens to the message?

This is the maximum size of a message that will be passed to this specific anti-spam module. If a message is greater than that, it will avoid this check, but will be passed to all the other.

Even if all anti-spam modules are avoided due to this, the message is still delivered.

This is a protection setting against DoS and a way to avoid wasting time and resources with techniques that do not apply on big data.

This setting is available to all the modules and should not be modified. This is an advanced setting that will work fine with the default value.

Generally, the default settings in the Anti-Spam part are quite fine and are optimized for the best efficiency with the databases provided in the Enterprise Edition of MailCleaner.

Whenever we feel, upon your analysis feedback, that these settings should be modified, we will let you know or take appropriate measures.

Content protection: Global settings

Questions:

"Send notice to administrator". When are these messages sent and what information do they contain?

This option will send a message to the specified address each time a virus or a dangerous content is being detected.

This option is disabled by default because it usually generates more noise that any precious information.

The information contains is the sender/recipient/subject of the message, and the reason why it has been blocked.

If the message was quarantined, the release information will also be included.

Services: Web interfaces

Questions:

"Allowed IP ranges". Can we block IP addresses from accessing the web interface?

- If we have understood things, then we can allow particular IP addresses.

Using the default 0.0.0.0/0 range, everybody will be able to connect to the web interfaces. This is usually what people want as they need to be able to access it from everywhere.

If you want to restrict it to some IP/Networks, then you have to put each exception in the box.

If you need more granularity and more advanced firewalling features, this should be applied in the firewall protecting MailCleaner.

Services: Database

Questions:

- How does this work? We assume that this allows remote access to a MySQL database?

Yes, this allows access to the MySQL database. But this should only be used for very specific cases and only where no other solution can be found.

If you need to programmatically interface with MailCleaner, you should definitively go with the API.

Accessing the database directly **cannot be supported by our support team**.

Services: API

Questions:

- May we have documentation for this?

The API manual can be found here: http://www.mailcleaner.net/downloads/MailCleanerAPI.pdf