INTRODUCTION

Mailcfg is a control panel for managing the mail server through an html interface. The system allows access to maintenance-modifications from three levels:

- User Level. Each holder of an email account can change the operating parameters corresponding to their account. You need an access password that the administrator will provide.

- Domain Administrator level. Since there can be multiple domains on a host, this structure is repeated in the mail administration. The domain administrator can access the user settings

- Server configurator level. Some important parameters that affect the global operation of the mail system can be managed from here. At this level, you have access to all the lower options.

As a whole, this mail system allows:

- Create pop3 and imap email accounts.
- Access through flat connections, SSL and STRATTLS.
- Setting flat or encrypted passwords (MD5 and NTLM)
- Account redirection- Input filters using white lists and blacklists.
- Autoresponders, global, or limited to whitelists.
- Outbound spam control through limiters per hour / day and month.
- Optional input filters for SPF, and several blacklist servers (bl).
- Statistics of use updated every few minutes.

USER ACCOUNTS

To access the maintenance of a user account, the access URL will normally be http: //mail.domain.tld or http://mail2.domain.tld. Normally to access this option you will need a web access password that will be supplied by the administrator.

Once inside, you must enter the email account and password (of those accounts) to access the user settings.

USER ACCOUNTS MANAGEMENT

On this screen you can modify the access password, account redirection and an autoresponder message.

To change the password it must be entered twice. The password must have at least eight digits.

All mail destined for this account can be redirected to another of the same domain, or of another other domain and server, by entering the desired destination address in the "Redirect to" box.

To generate an autoresponder message, you can fill in the available text box. It is recommended to use this option only with activated white lists, to avoid unwanted confirmations of active mail (For example, a spammer upon receiving this reply, will have the confirmation that the account is used, and will surely boost spam to this account).

When using this option you must take the following points into account.

- If the whitelist is not active, the autoresponder will go to all mail received, with the consequent spam reinforcement.

- If the white list is active, only users on this list will receive the autoresponder. This is the recommendation for normal use.

- Responses are managed by sender and day. This is a way to avoid the immediate

bounce, that if on the other side there is another autoresponder, it can lead to blocking the server by an endless loop. This means that a maximum of one response per day to the same sender is answered.

USER ACCOUNT SUMMARY

This screen will allow you to check the settings that you must put on your computer or mobile device.

Usually it is recommended to use a secure connection either STARTTLS or SSL. When a secure connection is established, all data is transmitted encrypted, including the password, so it is not necessary to use encrypted passwords on secure connections, but it is compatible.

Many mobile devices and some modern programs, such as Outlook or Thunderbird, intelligently manage the creation of a new account. This is perfectly valid and generally simple. However, in many cases, if you want to set up a pop account it is usually necessary to enter it manually.

When you register an account that will only be used on one device, you can use the IMAP protocol. However sharing IMAP accounts give problems with many mail client programs. On the contrary, if you want to use shared POP3 accounts it is very important that the delete box on the server is not checked when you delete the mail and check the delete box on the server after N days.

WHITE AND BLACK LISTS

Here you configure the black and white lists. Each list can be completed but it will be deactivated if the corresponding box indicates it.

Lists are a means of filtering incoming mail and are managed as follows:

First of all, for each incoming email, it is checked whether the sender's address is blacklisted. If yes, incoming mail is ignored.

Otherwise the white list is checked. If the sender appears on that list the email is accepted. Otherwise the email is rejected and optionally you can send

an email to the sender with the necessary instructions to be unlocked. By default after a clean installation this message is not sent and must be prepared in a personalized way for each installation with the appropriate indications.

The syntax for filling in the lists must specify a match per line, and can be a complete account or a domain. In this case it is recommended to put the @ symbol before.

DOMAIN ADMINISTRATION

Managing email accounts in a domain allows you to add new accounts, keep them and delete them. It also allows you to make king addresses of any of these accounts.

To access this maintenance enter the domain name and access password.

Once your credentials are accepted, you will have access to:

. Maintenance of domain user accounts.

. Maintenance of domain redirects.

. Modification of the access password.

DOMAIN ACCOUNTS

In this option you can add accounts accounts or change both the name of the account and the password. For security reasons the keys are not shown on the screen, but nevertheless for operability they can be seen momentarily by pressing the mouse button on the password box.

To add a new account you must indicate both the username and password. At this level, passwords do not have zero limitations. It is recommended to use passwords of six or more digits that have no relation to the username and that are not too simple.

You should not be mistaken and think that there is nothing interesting behind this email account and therefore there will be no interest from anyone in hacking it. The reality is that the majority of password thefts that occur in recent years are not intended to obtain data but access to an open gateway for mass spam.

To delete an account, simply delete the username and confirm the modification

using the record accounts button.

EMAIL REDIRECTS

Through this utility you can redirect email accounts. The redirection consists in alter the recipient of a certain email. You can redirect both accounts that have their own mailbox and others that do not. This means that a username can only be in domain accounts, it can only be in redirects or it can be simultaneously in both. In the latter case, redirection is imposed on the mailbox, but when the redirection is canceled, the mailbox is active again.

Of course, redirects must always correspond to the domain being managed, but the destination can be any valid email address.

PASSWORD CHANGE

With this option you can modify the access password for this maintenance (domain maintenance).

HOST CONFIGURATION

If you have a dedicated server, you can access this group of utilities that allow you to customize the overall functioning of the mail server.

Through these utilities you can:

. Add or remove new email domains.

. Manually set inbound filters that will allow you to block from an email address to a complete TLD (top level domains).

. Set maximum shipping limits per account as well as SPF filters and black lists.

. You will have access to a statistic with the latest available usage data.

DOMAINS MANAGEMENT

This option will allow you to add, modify or delete email domains. In the drop-down blind at the top of the panel you will have the list of domains currently in use. By selecting one of these pre-existing domains you will have the option to modify the data or completely cancel the domain.

To create a new domain, select NEW in the drop-down list, fill in the details and press the new button.

GLOBAL INPUT FILTER

This utility will allow you to exploit the internal filter of the server itself to eliminate spam. Although this option is mainly aimed at limiting access by domains, its powerful regex editing system allows you to go much further, allowing you to apply this advanced syntax for TLD domains or for other purposes.

If we do not use regex syntax, the system will match any of the lines that appear in the drop-down panel. This operation is very simple but it should be remembered that the coincidence may not be exactly what we expect. For example, let's imagine that we want to block a domain called test.com. If we add the test.com line as is, we will block any email in which this match is found, for example:

- test.comercial@gmail.com
- juan.lopez@mastest.com
- user@test.com

This inconvenient may be remedied simply by adding '@' in front of the domain.

However, if we want to block specific accounts, we will surely be forced to use regex. The following example serves as an illustration, and in it, the john@test.com account is blocked.

- j.john@test.com also user of the same server will be blocked
- john@test.com would work perfectly.

Among other things, the regex syntax allows you to indicate the beginning and end of the match. To indicate start we will use the combination of characters \. While to indicate final we will use the combination of characters \$

Also, in order to determine what the syntax used is regex, the entire set must be between '/' characters. Applying this syntax the example we saw earlier could be limited with all precision through the expressions:

- /\.john@test.com/ (Valid)
- /\.john@test.com\$/ (Better yet)

SPAM CONTROL (OUTGOING AND INCOMING

Now let's see how to have more control over sending and receiving emails. The first section of this option allows you to set the email delivery limits for each user account by hour, day and month.

These limits must be handled with extreme caution as it is the safeguard to avoid the massive launch of spam both motivated by theft of passwords, for any type of virus on users' computers or for any other reason.

In this sense it is important to know that with current modern technologies a single hacked account can send up to 10,000 emails per hour, more than enough to be detected that for many blacklist servers wich detect the activity of this server as a spammer.

At the bottom we have the possibility of activating or deactivating the SPF input filter, as well as several filters corresponding to blacklisted servers. Normally it is recommended to always use the SPF filter, and as for blacklists you can evaluate which ones interest you based on:

- spamhaus. Moderate blacklist very recognized among mail administrators.

- spamcop It is a moderate blacklist that has worked for many years.

- sorbs It is one of the most appreciated lists on the internet, although in some occasions it has included gmail as a bad reputation server which can cause us to stop receiving some emails.

- barracuda. It is one of the most restrictive internet lists. Including statesman as a filter ensures a minimum level of spam although emails could be lost.

STATISTICS

The mail system statistics will allow you to check the following data by email and day:

- Pop3_: number of POP3 connections made
- Imap_: number of IMAP connections made
- Sent: number of emails sent
- Bounc: number of shipments rejected (bounced)

- Defer: number of postponed shipments (deferred)
- Queue: number of shipments waiting (queued)
- PSent: reserved
- Reser: reservation
- Rejec: number of rejected shipments (reject)
- BList: number of incoming emails blocked by blacklists
- NoSPF: number of incoming emails blocked for breaching SPF criteria
- LostC: number of interrupted connections.

APENDIX

Real-time process: smtpfilter

. Spam out control

. Incomming mail:

.1 Check blacklist. Founded -> drop

.2 Check whitelist. Not found -> response with policy explanation (Delayed)

.3 Sent to recipient.

.4 Check autoresponder. -> Send response to sender

Deferred process: maillog

. Lock control.

ID: ctladdr=user@domain.tld -> counter -> lock if exceed

. Response not whiitelist.

ID: response to = sender from=user@domain.tld not whitelisted -> send if not previously done

. Autoresponse.

ID: response to = sender from=user@domain.tld autoresponse

ID: warning: Subject .... from -> send if not sent already