





Index

1. L'interface d'administration.....	3
1.1 Accès distant.....	3
1.2 Modification des paramètres de l'interface.....	3
2. La gestion du filtrage.....	5
2.1 Au niveau protocole.....	5
Les listes.....	8
2.2 Au niveau du filtrage antispam VadeRetro.....	10
Profil TAG.....	10
Profil QUARANTAINE.....	11
3 La gestion du routage.....	13
4 Le tableau de bord.....	14
4.1 le Dashboard global.....	14
4.2 Les compteurs.....	15
4.3 statistiques par domaine.....	16
5 La quarantaine.....	17
5.1 Administration.....	17
5.2 Les rapports	19
5.2.1 Le rapport administrateur.....	19
5.2.2 Le rapport utilisateur.....	19
6 Administration.....	21
6.1 Sauvegardes.....	21
7 Foire Aux questions.....	22
Comment fonctionne le support ?.....	22
Que faire en cas de panne ?.....	22
Puis-je créer mes propres règles de filtrage ?.....	22
Puis-je bloquer les Newsletters ?.....	22
Comment se passe l'échange de matériel en cas de panne matérielle ?.....	23

1. L'interface d'administration

1.1 Accès distant

L'interface d'administration du boîtier MailCube est accessible via votre navigateur web, à l'adresse :

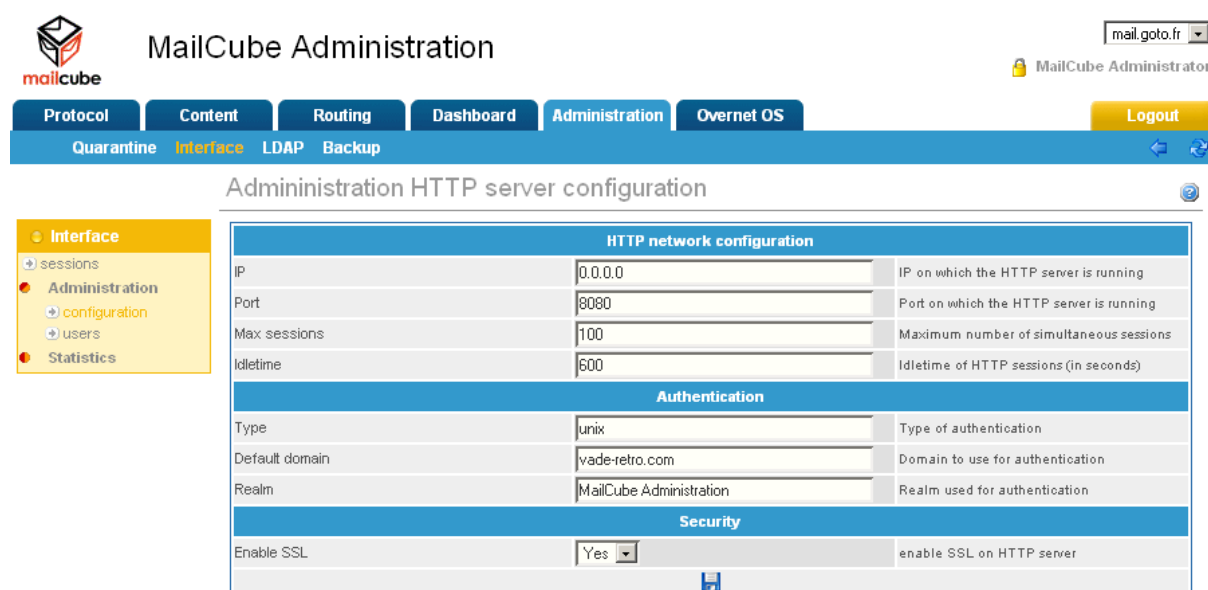
<https://ip-ou-nom-dns:8080/>

Un autre serveur web est en écoute sur le port 80 standard et en http, serveur sur lequel nous reviendrons après, car c'est lui va gérer l'administration des quarantaines pour les utilisateurs.

Vous arrivez donc sur une page d'authentification où les identifiants sont par défaut : vaderetro / vadebiz

1.2 Modification des paramètres de l'interface

Une fois que vous vous trouvez sur l'interface d'administration, vous pouvez modifier les options de ce serveur web, via l'onglet Administration/Interface, puis dans le cadre jaune à gauche : Administration => configuration



The screenshot shows the MailCube Administration web interface. At the top, there is a navigation bar with tabs for Protocol, Content, Routing, Dashboard, Administration, and Overnet OS. A 'Logout' button is visible on the right. Below the navigation bar, the main content area is titled 'Administration HTTP server configuration'. On the left side, there is a yellow sidebar menu with options: Interface (selected), sessions, Administration (with a sub-option 'configuration'), users, and Statistics. The main configuration area is divided into three sections: HTTP network configuration, Authentication, and Security. Each section contains several configuration fields with their current values and descriptions.

HTTP network configuration		
IP	0.0.0.0	IP on which the HTTP server is running
Port	8080	Port on which the HTTP server is running
Max sessions	100	Maximum number of simultaneous sessions
Idletime	600	Idletime of HTTP sessions (in seconds)

Authentication		
Type	unix	Type of authentication
Default domain	vade-retro.com	Domain to use for authentication
Realm	MailCube Administration	Realm used for authentication

Security		
Enable SSL	Yes	enable SSL on HTTP server

Vous pourrez changer ici le port d'écoute (8080), l'activation du SSL (https), ainsi que d'autres options

Toujours dans le cadre jaune de gauche, et dans la partie 'users', vous pourrez gérer les utilisateurs autorisés à se connecter à cette interface



Administration users

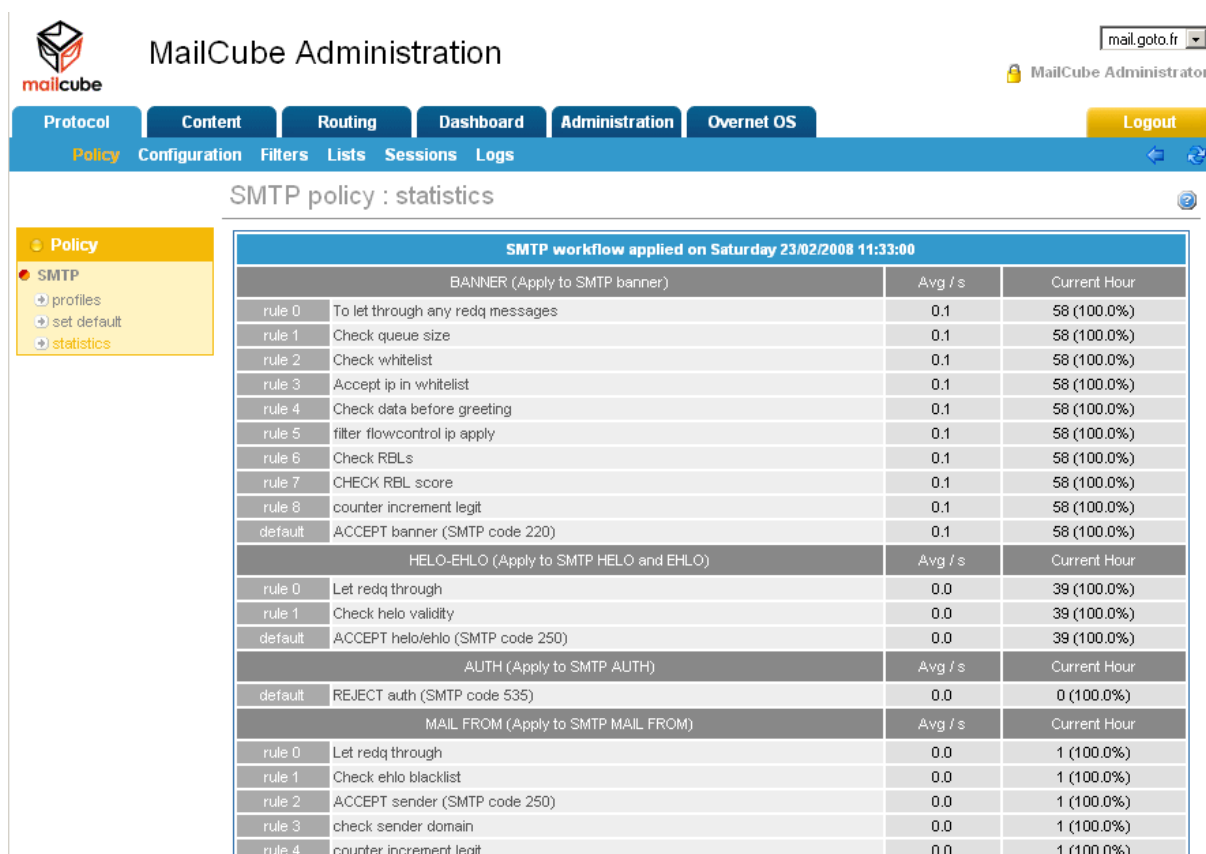
- Interface
- sessions
- Administration
 - configuration
 - users
- Statistics
 - configuration

List of users			
Login	Group	Name	Password
support	Administrator	Administration du support	*****
vaderetro	Administrator	MailCube Administrator	*****
	Administrator		

2. La gestion du filtrage

2.1 Au niveau protocole

Au niveau de l'interface, toute la configuration de la sécurité SMTP se trouve au niveau de l'onglet Protocol



The screenshot shows the MailCube Administration interface. The top navigation bar includes 'Protocol', 'Content', 'Routing', 'Dashboard', 'Administration', and 'Overnet OS'. The 'Policy' tab is active, showing a sidebar with 'SMTP' selected. The main content area displays 'SMTP policy : statistics' for Saturday 23/02/2008 11:33:00. The statistics are organized into four sections: BANNER, HELO-EHLO, AUTH, and MAIL FROM, each with a table of rules and their performance metrics.

SMTP workflow applied on Saturday 23/02/2008 11:33:00			
BANNER (Apply to SMTP banner)		Avg / s	Current Hour
rule 0	To let through any redq messages	0.1	58 (100.0%)
rule 1	Check queue size	0.1	58 (100.0%)
rule 2	Check whitelist	0.1	58 (100.0%)
rule 3	Accept ip in whitelist	0.1	58 (100.0%)
rule 4	Check data before greeting	0.1	58 (100.0%)
rule 5	filter flowcontrol ip apply	0.1	58 (100.0%)
rule 6	Check RBLs	0.1	58 (100.0%)
rule 7	CHECK RBL score	0.1	58 (100.0%)
rule 8	counter increment legit	0.1	58 (100.0%)
default	ACCEPT banner (SMTP code 220)	0.1	58 (100.0%)
HELO-EHLO (Apply to SMTP HELO and EHLO)		Avg / s	Current Hour
rule 0	Let redq through	0.0	39 (100.0%)
rule 1	Check helo validity	0.0	39 (100.0%)
default	ACCEPT helo/helo (SMTP code 250)	0.0	39 (100.0%)
AUTH (Apply to SMTP AUTH)		Avg / s	Current Hour
default	REJECT auth (SMTP code 535)	0.0	0 (100.0%)
MAIL FROM (Apply to SMTP MAIL FROM)		Avg / s	Current Hour
rule 0	Let redq through	0.0	1 (100.0%)
rule 1	Check ehlo blacklist	0.0	1 (100.0%)
rule 2	ACCEPT sender (SMTP code 250)	0.0	1 (100.0%)
rule 3	check sender domain	0.0	1 (100.0%)
rule 4	counter increment legit	0.0	1 (100.0%)

Dans une 1ere sous-rubrique 'Policy', vous retrouverez l'ensemble des règles de filtrage suivant chaque étape du protocole SMTP, suivi des statistiques de filtrage de la dernière heure.

Le profil livré par défaut avec le boîtier est fonctionnel pour la majorité des installations. Néanmoins vous avez la possibilité d'éditer les règles de filtrage. Pour cela, rendez vous dans la partie 'Profiles', et sélectionnez le profil actif. Vous allez donc arriver sur cette page :





BANNER (10)	HELO-EHLO (3)	AUTH (1)	MAIL FROM (6)	RCPT TO (5)	DATA (11)
[To let through any redq messages]					
rule 0	IF	OR	connection ip source [matches] [127.0.0.1]	OR	connection ip source [exists in list] [IP_whitelist]
	THEN		variable set [THIS_IS_FROM_REDQ] description [FP, report or access token from redq] type [integer] value [1]		ACCEPT connexion banner : SMTP code 220 - [ESMTP server ready]
[Check queue size]					
rule 1	IF		queues messages number [≥] [1000]		
	THEN		counter increment name [SMTP_BANNER_QUEUE_SIZE] description [Limit queue size]		wait seconds [3]
					FAILURE connexion banner : SMTP code 421 - [ESMTP server temporarily not available]
[Check whitelist]					
rule 2	IF		connection ip source [exists in list] [ip_whitelist]		
	THEN		variable set [wl] description [whitelist] type [integer] value [1]		
[Accept ip in whitelist]					
rule 3	IF		variable [wl] (integer) [=] [1]		
	THEN				ACCEPT connexion banner : SMTP code 220 - [ESMTP server ready]
[Check data before greeting]					












Chaque onglet reprend les étapes du protocole SMTP :

- BANNER : Initialisation de la connexion
- HELO-EHLO : Présentation mutuelle des interlocuteurs
- AUTH : Identification SMTP, non utilisée pour la Mailcube
- MAIL FROM : Déclaration de l'expéditeur
- RCPT TO : Déclaration du destinataire
- DATA : Transmission du message

Dans chaque onglet, vous retrouvez la liste des règles qui forment une procédure. Vous avez un contrôle total sur le filtrage et vous pouvez de créer des exceptions, renforcer le filtrage, créer du filtrage sur les destinataires, etc.

Prenons l'exemple sur une règle du protocole, à l'étape 'MAIL FROM' qui va permettre au filtrage de refuser les emails expéditeurs avec un domaine non-existant :

[check sender domain]	
rule 3	<p>IF NOT  smtp mailfrom domain is valid [MX or A]</p> <p>THEN</p> <ul style="list-style-type: none">  counter increment spam  counter increment name [SMTP_SENDER_BADDOMAIN] description [Unknown sender domain]  REJECT sender and CLOSE session : SMTP code 550 - [<\$_fromemail> sender rejected]

enhanced rule ▾	Rule description : check sender domain
[IF]	 ... [IF] select one condition to add ... +
NOT ▾	 smtp mailfrom domain is valid MX or A ▾ ✖
[THEN]	 ... [THEN] select one action to add ... +
	 counter increment spam ✖
	 counter increment name SMTP_SENDER_BADDOMAIN ✖
	 description Unknown sender domain ✖
	 ... [THEN] select one stop function ... ✔
	 REJECT sender and CLOSE session : SMTP code 550 - [<\$_fromemail> sender rejected] ✖
[ELSE]	 ... [ELSE] select one action to add ... +
	 ... [ELSE] select one stop function ... ✔
	

La plupart des règles sont composées en IF / THEN / ELSE.

Dans notre exemple, voici, francisé, ce que dit la règle :

SI domaine expéditeur NON valide au niveau MX/A
ALORS

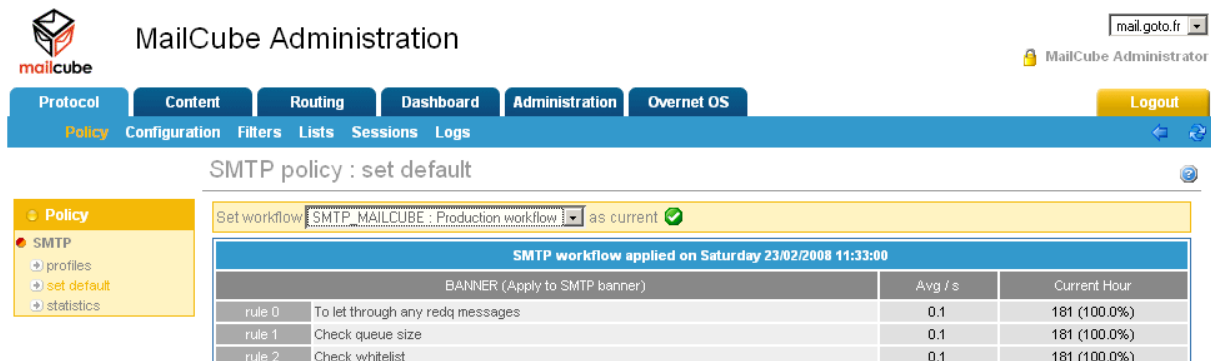
On incrémente le compteur général 'spam'

On incrémente un compteur spécial à cette règle

On refuse via un 'sender rejected', et on coupe la session

Attention !

Toutes modifications de règles du profil courant doivent entraîner une réactivation du profil, via le lien 'set default' présent dans le cadre jaune, bien sélectionner le profil qui correspond, et cliquer sur **as current** 



The screenshot shows the MailCube Administration web interface. The top navigation bar includes 'Protocol', 'Content', 'Routing', 'Dashboard', 'Administration', and 'Overnet OS'. The 'Administration' section is active, showing 'SMTP policy : set default'. A yellow box contains the text 'Set workflow SMTP_MAILCUBE : Production workflow as current' with a green checkmark icon. Below this, a table displays the SMTP workflow applied on Saturday 23/02/2008 11:33:00. The table has three columns: 'rule', 'description', 'Avg / s', and 'Current Hour'.

SMTP workflow applied on Saturday 23/02/2008 11:33:00			
BANNER (Apply to SMTP banner)			
rule 0	To let through any redq messages	0.1	181 (100.0%)
rule 1	Check queue size	0.1	181 (100.0%)
rule 2	Check whitelist	0.1	181 (100.0%)

Les listes

Les règles permettent l'usage de listes. On peut par exemple créer une règle autorisant l'envoi d'un mail sans le filtrer si l'expéditeur se trouve dans une liste 1 et le destinataire dans une liste 2.

Les listes peuvent contenir des adresses mails, des domaines, des adresses IP, des objets du message etc.

Vous trouverez ces listes au niveau de l'onglet Protocol, sous-rubrique 'lists' :



Lists Management

→ Lists → Edit list: Select list.. ▾

Lists	
sender_domain_whitelist	 
secured_relay	 
rcpt_domain_whitelist	 
rcpt_email_whitelist	 
ehlo blacklist	 
sender_email_whitelist	 
sender_email_blacklist	 
sender_domain_blacklist	 
ip_whitelist	 
	

Il existe plusieurs listes prédéfinies :

- sender_domain_whitelist : domaine pour lequel tous les mails sont acceptés
- sender_domain_blacklist : domaine pour lequel tous les mails sont refusés
- sender_email_whitelist : expéditeur pour lequel tous les mails sont acceptés
- sender_email_blacklist : expéditeur pour lequel tous les mails sont refusés
- rcpt_domain_whitelist : domaine destinataire sans filtrage
- rcpt_email_whitelist : adresse destinataire sans filtrage
- ip_whitelist : serveurs externe pour lequel tous les mails sont acceptés
- ehlo blacklist : présentation de serveurs refusées (permet de bloquer des machines infectées)
- secured_relay : adresses des serveurs de messagerie internes

Certaines listes, comme ehlo_blacklist et secured_relay ne présentent pas un intérêt immédiat et seront le plus probablement remplies par les techniciens de Goto Software en fonction de vos besoins (filtrage sortant, protection anti-deni de service etc.)

Vous pouvez ajouter facilement et dynamiquement les éléments dans ces listes déjà prédéfinies. Il faut indiquer un élément par ligne.

Si vous complétez une liste de noms de domaines, pas besoin d'indiquer le @ (mettez directement goto.fr au lieu de @goto.fr)

The screenshot shows the MailCube Administration interface. The top navigation bar includes Protocol, Content, Routing, Dashboard, Administration, and Overnet OS. The main menu includes Policy, Configuration, Filters, Lists, Sessions, and Logs. The current page is Lists Management, showing a dropdown for 'blacklist_email'. Below this, there are two panels: 'Current Items' and 'Add Items'. The 'Current Items' panel shows a table with 3 entries:

Item	Counter
info@cun.fr	1
invitation@venteprivee.com	1
jagent@route.monster.com	1

The 'Add Items' panel contains a text area with the following content:

```
spameur@poubelle.com
spam@spam.fr
```

2.2 Au niveau du filtrage antispam VadeRetro

Toute la partie configuration se trouve sous l'onglet Content (filtrage de contenu). Vous y retrouverez à la même manière qu'au protocole, une liste de profils de règles à activer.

Dans la sous-rubrique Policy, vous retrouverez les statistiques des différentes règles, et via la panneau jaune de gauche, les différents profils proposés :

The screenshot shows the MailCube Administration interface with the 'Policy' tab selected. The main content area displays 'CONTENT policy: profiles'. On the left, there is a sidebar with a yellow background containing the following items:

- Policy
- profiles
- set default
- statistics

The main content area shows a dropdown for 'Profile' and a table with the following entries:

Profile	Description
COITEHT_MAILCUBE_QUARANTINE	MailCube content workflow applied to USER QUARANTINE
COITEHT_MAILCUBE_TAG	MailCube content workflow applied to ***TAG***

2 profils sont livrés par défaut : une qui modifie le sujet des spams détectés (« taguage »), puis un 2nd qui gère une quarantaine.

Le fonctionnement des deux profils est proche : le moteur antispam VadeRetro analyse le message et fourni 2 variables : vrspamstate (0 mail légitime, 1 spam, 2 virus détecté par le moteur VadeRetro, 3 notification, 4 état d'un module externe) et vrspamscore (le « taux de spamicité » du message)

Par défaut, si le message est détecté comme virus, s'il a une alerte d'un module externe ou si son score de spamicité est supérieur à 1000, il est détruit.

Si le message a un score de spamicité compris entre 100 et 1000, son traitement sera lié au profil utilisé.

Profil TAG

Le profil TAG ne s'occupera que de taguer les spams de ***SPAM*** ou de ***VIRUS***, puis routera les messages vers votre serveur de messagerie.

Ce profil vous prive de la gestion des boîtes de quarantaine proposée par Mailcube : c'est à votre serveur de messagerie, aux logiciels de messagerie des utilisateurs ou aux utilisateurs eux-même de faire le tri.

Profil QUARANTAINE

Le profil QUARANTINE placera automatiquement les spams dans une zone de quarantaine, qui ne seront bien évidemment pas délivrés à votre serveur. Nous reviendrons dans une partie suivante sur le fonctionnement de cette quarantaine.

Le profil reprend donc et teste ces valeurs pour gérer les actions correspondantes :

rule 3	<p>[Check (vrspamstate = 1 && vrspamscore >= 100) = SPAM = USER QUARANTINE]</p> <p>IF</p> <ul style="list-style-type: none"> variable [vrspamstate] (integer) [=] [1] AND variable [vrspamscore] (integer) [>=] [100] AND variable [vrspamscore] (integer) [<=] [1000] <p>THEN</p> <ul style="list-style-type: none"> counter increment name [CONTENT_VADERETRO_SPAM_USER_QUARANTINE] description [CONTENT_VADERETRO_SPAM_USER_QUARANTINE] counter increment spam QUARANTINE message
rule 5	<p>[Check (vrspamstate = 1 && vrspamscore >= 1000) = SPAM = DROP]</p> <p>IF</p> <ul style="list-style-type: none"> variable [vrspamstate] (integer) [=] [1] AND variable [vrspamscore] (integer) [>=] [1000] <p>THEN</p> <ul style="list-style-type: none"> counter increment spam counter increment name [CONTENT_VADERETRO_DROP] description [CONTENT_VADERETRO_DROP] DROP message
rule 6	<p>[Check vrspamstate = 2 = VIRUS = USER QUARANTINE]</p> <p>IF</p> <ul style="list-style-type: none"> variable [vrspamstate] (integer) [=] [2] <p>THEN</p> <ul style="list-style-type: none"> counter increment virus counter increment name [CONTENT_VADERETRO_VIRUS_USER_QUARANTINE] description [CONTENT_VADERETRO_VIRUS_USER_QUARANTINE] message subject [prepend with] [***Virus***] DROP message
rule 7	<p>[Check vrspamstate = 3 = BOUNCE = USER QUARANTINE]</p> <p>IF</p> <ul style="list-style-type: none"> variable [vrspamstate] (integer) [=] [3] <p>THEN</p> <ul style="list-style-type: none"> counter increment name [CONTENT_VADERTRO_BOUNCE_USER_QUARANTINE] description [CONTENT_VADERTRO_BOUNCE_USER_QUARANTINE] counter increment spam message subject [prepend with] [***Bounce***] QUARANTINE message
rule 8	<p>[counter increment legit]</p> <p>APPLY</p> <ul style="list-style-type: none"> counter increment legit
default	<p>[ROUTE message]</p> <p>APPLY</p> <ul style="list-style-type: none"> ROUTE message

En résumé, suivant le paramétrage par défaut :

- ⇒ Tout spam léger sera placé en quarantaine ou tagué
- ⇒ Tout spam dur sera supprimé
- ⇒ Tout virus sera supprimé
- ⇒ Toute notification sera placée en quarantaine/taguées si l'option de protection contre les notifications est mise en place.
- ⇒ Le reste sera routé normalement vers le serveur de messagerie

 Attention !

Tout comme pour le filtrage protocolaire, Vous devrez réactiver le profil après toute modification.

Vous trouverez ensuite la configuration du moteur VadeRetro dans la partie 'VadeRetro' sous l'onglet 'Content'. Vous pourrez alors spécifier :

- l'activation ou non du moteur antivirus
- la mise en place de protection contre les notifications.
- le full scoring (qui permet de donner un score plus précis sur les spams)
- l'accentuation des jeux de caractères étrangers dans le cas où vous n'êtes pas sujet à en recevoir
- la licence à utiliser (obligatoire pour la mise à jour de la librairie antispam)
- un proxy pour la sortie sur le 80 pour le rapatriement des mises à jour
- l'intervalle de mise à jour

MailCube Administration mail.goto.fr
MailCube Administrator

Protocol | Content | Routing | Dashboard | Administration | Overnet OS | Logout

Policy | Filters | Lists | **Vaderetro** | Logs

Vaderetro

Status		
Current version	Vade Retro 01.243.02 AV+AS	
Configuration parameters		
Perform anti-virus checks	<input type="text" value="No"/>	
Perform anti-bounce (delivery notification) checks	<input type="text" value="No"/>	
Perform full scoring (prefer exact score over speed)	<input type="text" value="Yes"/>	
Ignore Cyrillic charsets in incoming messages	<input type="text" value="No"/>	
Ignore Chinese, Korean and Japanese charsets in incoming messages	<input type="text" value="No"/>	
License	<input type="text" value="xxxxxxx"/>	Required to download updates
Http proxy	<input type="text"/>	Optional
Auto update interval (min)	<input type="text" value="240"/>	0 to disable auto update
Update management		
Status	Up to date	
Last check for update	Mon, 25 Feb 2008 19:51:26 +0100	
Previous version	Vade Retro 01.243.01 AV+AS	

Vous trouverez enfin en bas de page le statut de la mise à jour automatique.

3 La gestion du routage

Le MailCube possède sa propre table de routage IP pour chaque domaine. Cette configuration est gérée à l'onglet Routing.

C'est une configuration à faire à l'installation du boîtier, et nécessite d'être maintenue à jour pour l'ajout/suppression de domaine de réception, ou encore la modification de l'architecture de votre réseau visant votre (ou vos) serveur(s) de messagerie.

La table de routage peut contenir des entrées simples (1 domaine vers 1 IP), ou des configurations plus avancées. Elle peut servir de load balancing entre 2 serveurs (même domaine pour 2 IP différentes) ou de backup (même domaine, IP différentes mais avec une priorité différente pour chaque IP de serveur de messagerie).

Dans le cas où tous vos domaines sont gérés uniquement par un seul et même serveur, vous pouvez n'ajouter qu'une seule avec comme domaine '*' (étoile) vers l'IP de votre serveur.

The screenshot shows the MailCube Administration interface. At the top, there is a logo for MailCube and the text "MailCube Administration". A dropdown menu shows "mail.goto.fr" and the user is identified as "MailCube Administrator". Below this is a navigation bar with tabs for "Protocol", "Content", "Routing", "Dashboard", "Administration", and "Overnet OS". A "Logout" button is also present. Underneath the navigation bar, there are links for "Configuration", "Sessions", and "Logs". The main content area is titled "SMTP routing table configuration". On the left, there is a sidebar menu with "Configuration" expanded, showing sub-items: "SMTP", "protocol", "extensions", "routing table", and "parameters". The "SMTP" sub-item is selected. The main table displays the following data:

ID	Domain	NB IPs	TTL	Outgoing SMTP server	Priority	
0	funbridge.fr	1	86400	192.168.10.202	10	✖
1	goto.fr	2	86400	192.168.10.201	10	✖
				192.168.10.202	15	✖
0			86400	0.0.0.0	10	+

4 Le tableau de bord

4.1 le Dashboard global

Le tableau de bord (onglet Dashboard) vous donnera les stats sur votre flux de messagerie. Reprenons un exemple :

The screenshot shows the MailCube Administration interface. At the top, there's a navigation bar with tabs for Protocol, Content, Routing, Dashboard (selected), Administration, Overnet OS, and Logout. Below the navigation bar, the 'Global Dashboard' is displayed for the date '10 February 2009'. The dashboard is divided into several sections:

- Incoming:** # connections received: 274270, Average # connections / s: 6.9, Average session time: 4.6 s.
- Outgoing:** # connections initiated: 36223, Average # connections / s: 0.9, Average session time: 43.7 s.
- Protocol workflow:** SMTP (73.9%), BANNER (73.5%), HELO/EHLO (0.1%), AUTH (0.0%), MAIL FROM (2.6%), RCPT TO (0.2%), DATA (0.0%).
- Content workflow:** # Messages received: 90093, # Messages stored: 0, # Messages dropped: 69611.
- Routing workflow:** # Messages sent: 69365, Volume total sent: 3157.8 MB, # Messages deleted from queue: 0.
- Global filtering:** 96.6%.
- Transit time:** Average transit time: 110.7 s.

Vous trouverez à gauche toute la partie 'filtrage protocolaire' : nombre de connexions reçues, nombre de connexions persistantes au fil des étapes du protocole, le nombre de connexions validés, poids, etc. Un taux de filtrage est d'or et déjà donné : ici un peu plus de 96%.

Au centre, la partie 'Content' qui correspond au filtrage antispam VadeRetro, où on peut voir le nombre de messages total à traiter, le nombre de messages ayant été mis en quarantaine (stored) et détruits (dropped), ainsi qu'un taux de filtrage ne concernant que la partie 'Content'.

Enfin, une partie Routing où nous trouverons le nombre de messages retransmis au serveur de messagerie en aval, ainsi que le poids du flux.

Le dashboard donne enfin un taux de filtrage global, qui reprend l'ensemble des statistiques et permet de justifier l'efficacité du boîtier.

D'autres statistiques plus avancées sont disponibles sous l'onglet Dashboard, parmi lesquelles nous insisterons sur la partie 'counters'.

4.2 Les compteurs

Cette partie va nous donner des indications sur des compteurs spécifiques, permettant de visualiser le nombre d'attaques sur telle ou telle partie du filtrage.

Penons un exemple :

Workflow Counter	Description	Value
Filtering rate		
SMTP filtering rate		88.4 %
CONTENT filtering rate		86.2 %
GLOBAL filtering rate		98.4 %
Other workflow counters		
CONTENT_VADERETRO_DROP	CONTENT_VADERETRO_DROP	16
CONTENT_VADERETRO_SPAM_USER_QUARANTINE	CONTENT_VADERETRO_SPAM_USER_QUARANTINE	9
CONTENT_VADERETRO_VIRUS_USER_QUARANTINE	CONTENT_VADERETRO_VIRUS_USER_QUARANTINE	0
CONTENT_VADERETRO_BOUNCE_USER_QUARANTINE	CONTENT_VADERETRO_BOUNCE_USER_QUARANTINE	0
SMTP_BANNER_CDBG	Reject data before greeting	1
SMTP_BANNER_QUEUE_SIZE	Limit queue size	0
SMTP_BANNER_RBL	Reject based on RBLs	0
SMTP_DATA_BADATTACHMENTTEXT	Drop message based on attachment extension	0
SMTP_DATA_BL	nbre de domaines/emails en blacklist	0
SMTP_DATA_OUT_MAILS	Mails sortants	0
SMTP_DATA_RCPT_DOMAIN_VWL	SMTP_DATA_RCPT_DOMAIN_VWL	0
SMTP_DATA_RCPT_EMAIL_VWL	SMTP_DATA_RCPT_EMAIL_VWL	0
SMTP_DATA_SENDER_DOMAIN_VWL	SMTP_DATA_SENDER_DOMAIN_VWL	0
SMTP_DATA_SENDER_EMAIL_VWL	SMTP_DATA_SENDER_EMAIL_VWL	0
SMTP_HELLO_DYNPOOL	Hello host looks like a dynamic pool	2878
SMTP_RCPTTO_CHECK_RCPTTO	nbre de dest invalide sur exchange	11
SMTP_RCPT_UNKOWN	SMTP_RCPT_UNKOWN	222
SMTP_SENDER_BADDOMAIN	Unknown sender domain	0
SMTP_SENDER_HELLO_BLACKLIST	hello blacklisted	0

Nous retrouvons nos taux de filtrage, mais plus important : les compteurs présents dans les règles. Il ya en général un compteur spécifique pour chaque règle de rejet ou d'exceptions.

On peut voir ici qu'il y a eu 16 suppressions de spams, et 9 mises en quarantaine. A coté de cela, nous avons eu un peu plus de 2800 connexion provenant d'IP dynamique, 222 destinataires avec un domaine non géré par le boîtier, et 11 rejets de destinataire invalide via une règle de vérification des destinataires.

4.3 statistiques par domaine

Dans la sous-rubrique 'domains' de l'onglet Dashboard, vous trouverez des stats par domaines.

Ce tableau vous indique le nombre de mail reçus, de spams mis en quarantaine et supprimés, et finalement le nombre de mails légitimes routés vers votre serveur, et cela pour chaque domaine :

mailcube Administration mail.goto.fr
MailCube Administrator

Protocol Content Routing Dashboard Administration Overnet OS Logout

Global Incoming Processing Outgoing Counters Domains Sender Export

Domains Dashboard

daily view on 04 January 2008 at 00:30

Domains dashboard : daily view for 04 January 2008									
Domain	Received	Volume	Exploded	Refused	Dropped	Stored	Bounced	Sent	Volume
no-domain.com	0	0 Bytes	0	0	0	0	0	0	0 Bytes
test.com.fr	16	108.1 KB	16	0	4	4	0	8	88.0 KB
test.com.fr@info	0	0 Bytes	0	0	0	0	0	0	0 Bytes
test.com.fr	0	0 Bytes	0	0	0	0	0	0	0 Bytes
others	0	0 Bytes	0	0	0	0	0	0	0 Bytes

5 La quarantaine

5.1 Administration

L'administrateur doit configurer lors de sa première utilisation quelques paramètres au niveau du serveur de quarantaine.

Pour cela, rendez-vous dans dans l'onglet 'Administration', sous-rubrique 'quarantine'. Vous retrouverez alors ce panel :

The screenshot shows the MailCube Administration web interface. At the top, there is a navigation bar with tabs for Protocol, Content, Routing, Dashboard, Administration (selected), and Overnet OS. A 'Logout' button is visible on the right. Below the navigation bar, the page title is 'Mailcube Quarantine Administration'. The main content area is divided into sections:

- Quarantine limits:** Contains two input fields: 'Maximum size (Ko/user):' with the value '10000' and 'Maximum no. of messages (msg/user):' with the value '1000'.
- Purge & Reporting:** Contains three input fields: 'Delete messages older than (days):' with the value '30', 'Preferred purge & reporting time (HH:MM):' with the value '03:00', and 'Send global admin reports to address:' with the value 'admin@goto.fr'. There are two checked checkboxes: 'Send reports to each user' and 'Send global admin reports to address:'.
- Immediate actions:** Contains two buttons: 'Quarantine user list - Enter' and 'Launch all purge & reporting - Now!'.

A 'Save' button is located at the bottom of the 'Purge & Reporting' section. The version information 'redq v1.58 (Oct 19 2007 15:02:18)' is displayed in the bottom right corner.

Chaque boîte aux lettres (BAL) possède son quota sur la quarantaine, afin de ne pas saturer l'espace disque. Vous réglerez 2 quotas ici : 1 concernant la taille (par défaut 10 Mo) et un 2nd pour le nombre de messages (1000 messages).

Vous trouverez ensuite des options globales, comme la durée de rétention, l'heure de la purge et d'envoi des rapports, ainsi que le choix d'envoyer ou non des rapports à chaque utilisateur, en leur donnant ainsi la main sur leur quarantaine, mais aussi d'activer ou non le rapport administrateur. Nous reviendrons un peu plus loin sur ces rapports...

Deux boutons sont présents, 'launch all purge and reporting now' vous permet de lancer la même action effectuée toutes les nuits à 3h du matin : la purge suivant la rétention et l'envoi des rapports, ainsi que le bouton 'quarantine user list', qui vous emmènera dans la quarantaine globale :



Mailcube Quarantine Administration

contact@	Enter	Send token
@	Enter	Send token
@	Enter	Send token
@	Enter	Send token

Deux choix possibles :

- Enter : entrer dans la quarantaine de l'utilisateur
- 'Send Token' : envoyer un jeton d'accès à l'utilisateur

Vous pouvez alors soit consulter la quarantaine de l'utilisateur et visualiser tous ses spams, ou lui donner accès à sa quarantaine. De cette manière, il devient complètement autonome, et peut gérer ses relâchements de spams, ses whitelists personnelles, etc.



Mailcube Quarantine Administration

Quarantaine e-mail de contact@

Tous

 contact @ @ 9%

Date	Nom de l'expéditeur	Adresse de l'expéditeur	Objet	Taille	Score
<input type="checkbox"/> 2008/02/25 20:57	peer	usrmoderator@nmconsult.com	*** SPAM *** It no dietary	3K	780
<input checked="" type="checkbox"/> 2008/02/25 13:58	Valerie Cameron	gottfried@jojomail.com	*** SPAM *** You rich	2K	1123
<input checked="" type="checkbox"/> 2008/02/25 11:45	La Scala Club	immortal@linuxmail.org	*** SPAM *** Déposez 93 Euro et jouez avec 200 Euro!	4K	620
<input type="checkbox"/> 2008/02/25 09:57	Lynne M. Leach	lynne_leach_zs@qualor.com	HugeDiscountWatches, nRolex (DatejustSport), Bell & Ross, LV & Guc	2K	1003
<input type="checkbox"/> 2008/02/25 09:22	Pearlie Graves	pearliegraves_lf@peppercorn.com	*** SPAM *** The World Most Effective PenisLonger Pill Is Now Available! 3wxg2i	2K	1323
<input type="checkbox"/> 2008/02/25 07:52	Aubrey Puckett	apuckett_yd@beacon.ca	*** SPAM *** The World Most Effective PenisLonger Pill Is Now Available! 0krdg5	2K	816
<input type="checkbox"/> 2008/02/25 06:28	Leonardo Wall	leonardo.wall_ht@technolution.com	*** SPAM *** The World Most Effective PenisLonger Pill Is Now Available! 2wgbkg	2K	816
<input type="checkbox"/> 2008/02/25 04:48	Raymundo Burger	raymundo.burger_pd@wanadoo.fr	*** SPAM *** Add up to 4 inches to yours penis lteh1e	2K	1330
<input type="checkbox"/> 2008/02/24 21:09	Addie Kern	addie.kern_jc@vpi.net	*** SPAM *** 88% Off Swiss-MadeRolex, Omega, Panerai, Chanel, 100% Satisfaction	2K	1003

Mode consultation par l'administrateur

Tous

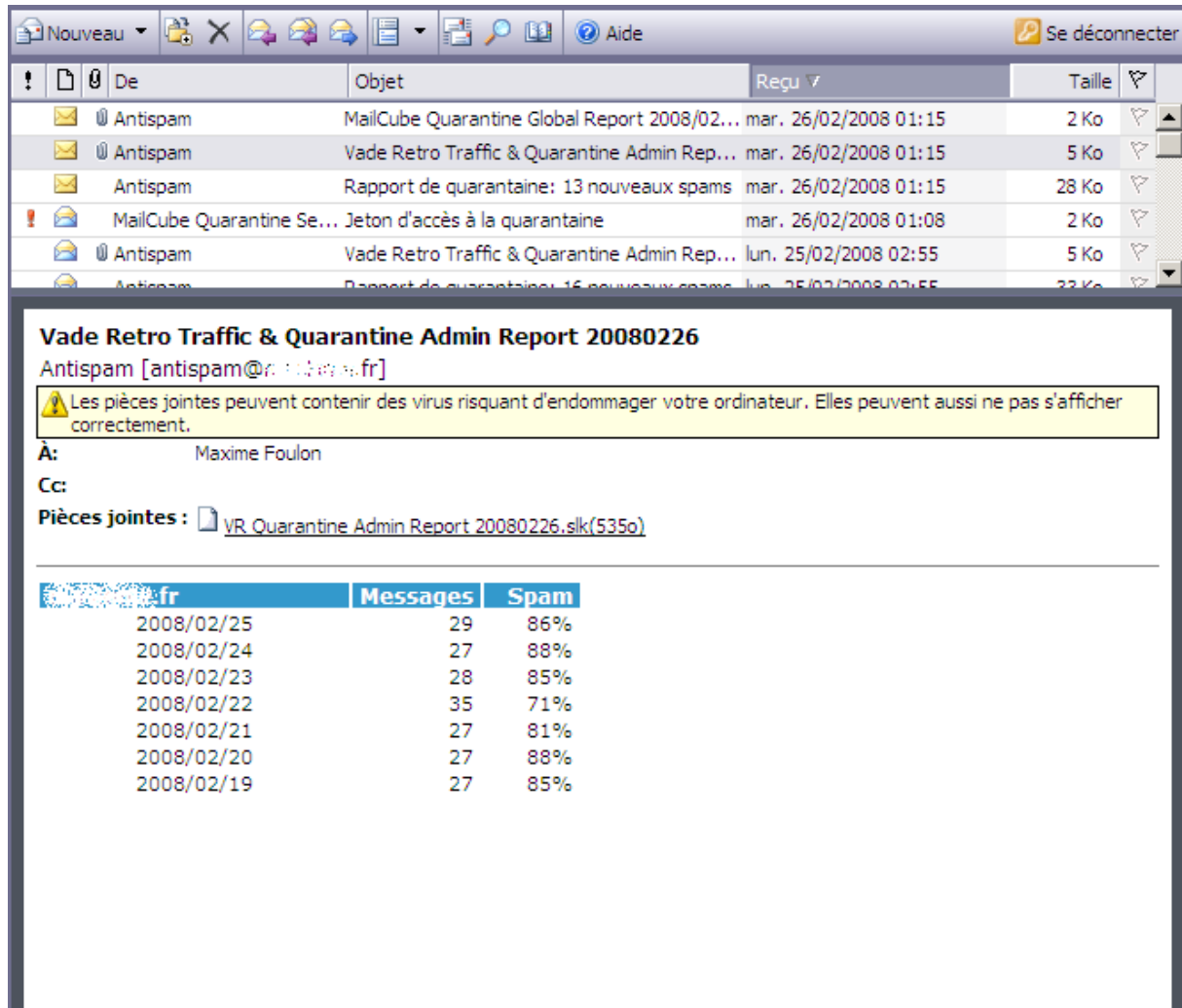
 @ 0%

Date	Nom de l'expéditeur	Adresse de l'expéditeur	Objet	Taille	Score
<input type="checkbox"/> 2008/01/30 16:08	cderostand@venteprivee.com	invitation@venteprivee.com	Diesel et 55DSL et Jalla vendredi 1er fvrier chez vente-privee.com	9K	0
<input type="checkbox"/> 2008/01/29 21:30	cderostand@venteprivee.com	invitation@venteprivee.com	Triumph et Sinquanone jeudi 31 janvier chez vente-privee.com	9K	0
<input type="checkbox"/> 2008/01/28 15:15	cderostand@venteprivee.com	invitation@venteprivee.com	Alain Figaret et Monix mercredi 30 janvier chez vente-privee.com	9K	0
<input type="checkbox"/> 2008/01/27 15:25	cderostand@venteprivee.com	invitation@venteprivee.com	Jean-Claude Biguine make-up & shampooing mardi 29 janvier chez vente-privee.c	7K	0
<input type="checkbox"/> 2008/01/26 15:38	cderostand@venteprivee.com	invitation@venteprivee.com	Alain Weiz et Jules Destroyer lundi 28 janvier chez vente-privee.com	9K	0

Mode consultation par l'utilisateur

5.2 Les rapports

5.2.1 Le rapport administrateur



The screenshot shows an email client window with a list of emails. The selected email is titled "Vade Retro Traffic & Quarantine Admin Report 20080226" from "Antispam [antispam@n...:fr]". A warning message states: "Les pièces jointes peuvent contenir des virus risquant d'endommager votre ordinateur. Elles peuvent aussi ne pas s'afficher correctement." The sender is "Maxime Foulon". The attachment is "VR_Quarantine_Admin_Report_20080226.slk(535o)".

fr	Messages	Spam
2008/02/25	29	86%
2008/02/24	27	88%
2008/02/23	28	85%
2008/02/22	35	71%
2008/02/21	27	81%
2008/02/20	27	88%
2008/02/19	27	85%

Il reprend sur une fenêtre de 7 jours les dernières statistiques en matière de filtrage antispam, c'est-à-dire le nombre de messages arrivés pour être filtrés, et le pourcentage de spams recensés.

Vous avez également en PJ du mail un fichier de type .slk (<http://fr.wikipedia.org/wiki/SYLK>) qui vous donnera des statistiques sur l'occupation de la quarantaine pour chaque BAL.

5.2.2 Le rapport utilisateur

En effet, s'il est activé, les utilisateurs vont recevoir un rapport journalier, leur listant les spams reçus :


Nouveau Se déconnecter

De	Objet	Reçu	Taille
Antispam	MailCube Quarantine Global Report 2008/02/26 01:19	mar. 26/02/2008 01:15	2 Ko
Antispam	Vade Retro Traffic & Quarantine Admin Report 20080226	mar. 26/02/2008 01:15	5 Ko
Antispam	Rapport de quarantaine: 13 nouveaux spams	mar. 26/02/2008 01:15	28 Ko
MailCube Quarantine Server	Jeton d'accès à la quarantaine	mar. 26/02/2008 01:08	2 Ko
Antispam	Vade Retro Traffic & Quarantine Admin Report 20080225	lun. 25/02/2008 02:55	5 Ko
Antispam	Rapport de quarantaine: 16 nouveaux spams	lun. 25/02/2008 02:55	22 Ko

Rapport de quarantaine: 13 nouveaux spams
 Antispam [antispam@...]

Afin de préserver votre confidentialité, les liens vers des images, des sons ou d'autres contenus externes dans ce message ont été bloqués. [Cliquez ici pour débloquer le contenu.](#)

A: Maxime Foulon
 Cc:

Occupation de la quarantaine :  14%

Pour consulter votre quarantaine, veuillez [cliquer ici](#).
 13 nouveaux spams, par ordre croissant de spammité :

Date	Nom de l'expéditeur	Adresse de l'expéditeur	Objet	Taille
2008/02/25 04:36	Barro	galen@neste.com	*** SPAM *** FW[3]:	3K
2008/02/25 05:40	pig Addison	_emenvaas@RealityPump.pl	*** SPAM *** Girls will never look at you the same way again.	3K
2008/02/25 08:33	kele shlomo	-ganz@adhes.com	*** SPAM *** Perfectly crafted luxury timepieces	5K
2008/02/25 10:01	bald catherin	jrhackett@netcom.com	Hermes	4K
2008/02/25 10:17	vaigra	tohru@yahoo.com	*** SPAM *** Save 85% on your drugs. Coupon #hdjff	2K
2008/02/25 10:33	Magic Jackpot	HaleyPresley@mailAccount.com	La rencontre du jeu et de la magie	3K
2008/02/25 12:37	arie guenter	-ado2@adamsgolf.com	*** SPAM *** Meds Coupon for m.foulon	4K
2008/02/25 13:30	Toner Services via eBuyClub	nepasrepondre@ebuyclub.com	maskime, votre cadeau est arriv	5K
2008/02/25 16:43	clarke play	jtjmm@att.net	*** SPAM *** Breitling	4K
2008/02/25 19:56	lock luiz	-ganz@adhes.com	*** SPAM *** Re:Freak the girls out with your gigantic SCHLONG!	11K
2008/02/25 22:32	Magic Jackpot	PatricaBoston@ev.net	La rencontre du jeu et de la magie	3K
2008/02/25 23:06	cassius gretchen	-ganz@adhes.com	*** SPAM *** She will get loads of pleasure with this!	3K

Ils pourront alors vérifier les spams arrêtés, les visualiser directement (via un lien sur la ligne du spam qui renvoie à un pop-up, ou accéder directement sur leur interface en web (cf. dernière photo du 5.1)

6 Administration

6.1 Sauvegardes

Il est possible de créer des sauvegardes de la configuration de l'appliance.

Vous devez pour cela vous rendre dans l'onglet 'Administration', section 'Backup'.

MailCube Administration

lxmail01.goto.fr | Support Goto Software

Protocol Content Routing Dashboard Administration Overnet OS Logout

Quarantine Interface LDAP Backup

Backup

Available backups			
Server name	Cluster ID	Version	Date
lxmail01.goto.fr	1	2.4.19vr	Tuesday 10/03/2009 15:47:47
lxmail01.goto.fr	1	2.4.19vr	Monday 21/07/2008 15:28:56

Backup current configuration

En cliquant sur 1 vous générez un fichier de sauvegarde qui apparaîtra dans la liste.
En cliquant sur 2 vous restaurez l'image de la sauvegarde.

Le support des sauvegardes (disque dur, clef USB etc.) peut être personnalisé via l'onglet 'OvernetOS', section 'Internals' et 'parameters' dans le menu.

La valeur à modifier est 'backupdev' et il s'agit du fichier symbolisant le périphérique dans le système d'exploitation. Le support Goto peut vous aider à connaître sa valeur.

7 Foire Aux questions

Comment fonctionne le support ?

Vous disposez d'un interlocuteur technique privilégié chez Goto Software. Si ce n'est pas le cas, contactez le commercial qui s'occupe de vous. Vous devez avoir le numéro de ligne directe ainsi que l'adresse de votre interlocuteur technique.

Cette personne suivra votre dossier : En cas de panne ou de question technique, c'est la première personne à contacter.

Que faire en cas de panne ?

Tout d'abord ne redémarrez jamais la Mailcube sans entrer en contact avec le support Mailcube.

Si vous avez redémarré la Mailcube, même si ça a résolu le problème, prévenez le support Mailcube.

Parfois des interventions à distances seront nécessaires. Il existe deux modes : SSH et NetViewer.

SSH est la solution privilégiée. Elle nécessite une ouverture dans votre firewall pour permettre à votre interlocuteur de se connecter sur le port 22 de la MailCube depuis Internet.

NetViewer est une solution plus lente, nécessitant la prise en main d'un poste client sur votre réseau. Un client NetViewer peut être téléchargé à l'adresse <http://www.goto.fr/demo/client.exe>

Puis-je créer mes propres règles de filtrage ?

Oui. Il faut que vous soyez conscients qu'il s'agit de modifications sensibles : une erreur peut entraîner des dysfonctionnements et la perte de mails.

Si vous avez le moindre doute sur l'opération, contactez le support Mailcube afin qu'il regarde avec vous ce que vous souhaitez faire et comment y parvenir.

Puis-je bloquer les Newsletters ?

Oui. Néanmoins, pour les Newsletters françaises, les liens de désinscriptions sont la méthode la plus efficace pour être débarrassés de l'abonnement.

Le rôle de la Mailcube est de filtrer les spams (messages non-sollicités). Les newsletters nécessite un abonnement : soit en renseignant son email dans un formulaire d'abonnement, soit en cochant la case pour recevoir des offres commerciales lors de l'inscription à un site (ou tout moyen similaire).

Il est important de le comprendre : ***Les newsletters ne sont pas du spam.***

Le blocage des Newsletters n'est pas toujours évident : l'expéditeur qui apparaît dans le logiciel de messagerie ne correspond pas toujours à celui indiqué dans l'échange SMTP. Hors c'est l'expéditeur indiqué dans l'échange SMTP qui est utilisé dans les listes blanches et noires.

Comment se passe l'échange de matériel en cas de panne matérielle ?

Si, après avoir appelé le support Mailcube, il apparaît que votre matériel est en panne, une procédure d'échange se met en place.

Le technicien Goto Software vous enverra par fax un bon pour accord pour le retour de la Mailcube pour maintenance. Une fois ce bon complété et retourné vous pouvez retourner le matériel à Goto Software avec un numéro de dossier qui vous aura été communiqué. Une fois le matériel reçu, Goto Software s'engage à réparer votre matériel et à vous retourner sous 48 heures votre Mailcube fonctionnelle ou un Mailcube de remplacement.

Si vous avez pris l'option d'échange anticipé, la mailcube de remplacement vous est immédiatement expédiée, sans attendre le retour de la précédente. Selon le délais disponible avant l'expédition, la mailcube sera préconfigurée ou non. Si elle n'a pas pu être préconfigurée, un technicien vous accompagnera pour le paramétrage une fois que vous aurez reçu le matériel.

Vous aurez ainsi dans la plus courte possible du filtrage antispam, là où la procédure classique peut prendre jusqu'à 5 jours ouvrés