



MailProve Super Blacklist

Service Overview

Prepared by:

Mail Prove Limited

July 5, 2004

Setting the Anti-spam standard in Asia

Mail Prove Limited

Unit 806, Cyberport 1
100 Cyberport Road
Pokfulam, Hong Kong

郵盾亞洲有限公司

香港薄扶林
數碼港道100號
數碼港1座806室

Tel 電話 (852) 3105 2920

Fax 傳真 (852) 3105 2926

Email 電郵 info@MailProve.com

www.MailProve.com

CONTENTS

MAILPROVE SUPER BLACKLIST SERVICE.....	3
A. How Does The Service Work?.....	3
B. Features for Service Providers.....	4
C. Platforms Supported.....	4
D. Hardware and Software Requirements.....	4
E. “Super Blacklist” Features.....	4
F. MailProve Infrastructure.....	5
G. Support.....	5
FREQUENTLY ASKED QUESTIONS (FAQ).....	6
1. What is the response time of the MTA when using MailProve Super Blacklist?.....	6
2. How up-to-date is MailProve’s Super Blacklist?.....	6
3. What is the accuracy of spam blocking?.....	6
4. How do we tackle Asia specific spam?.....	6
5. Can an email administrator check the blocking status of their mail server or MTA?.....	6
6. Does MailProve “read” the content of my email?.....	7
7. How do we treat spammers?.....	7
8. What is our anti-spam strategy?.....	7
9. Can customers control their own blacklist and whitelist?.....	7
10. What happens when a large email system is blocked? Will that block all email from that location?.....	7

MailProve Super Blacklist Service

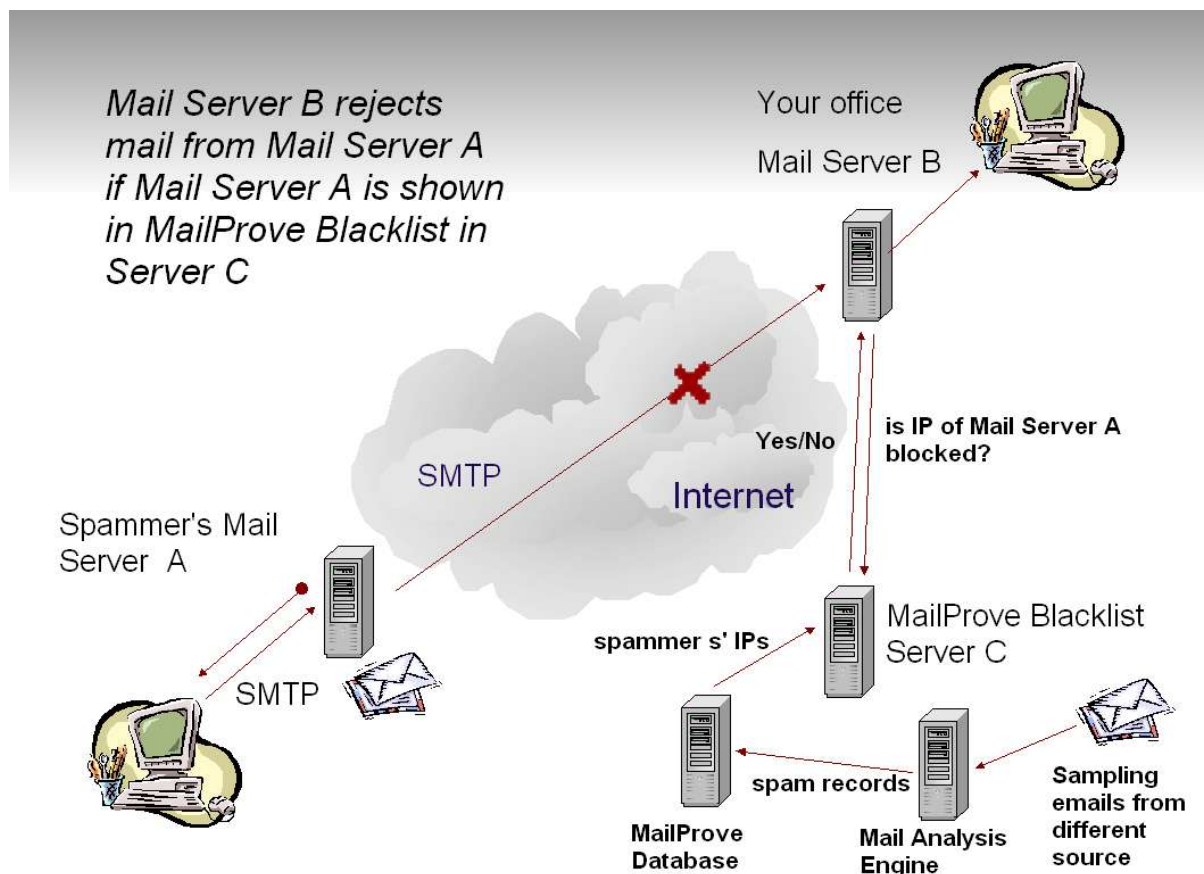
The **MailProve Super Blacklist Service** is a real-time IP address blacklist service developed on Internet and open-source technology. It has been **extensively enhanced** to include many features that are specific to the requirements of **Enterprises** and **Service Providers**.

The Service provides real-time blocking decisions for legitimate email servers or MTAs against spamming email servers, virus sending servers and access pools of ISPs. We block spam on behalf of our customers wherever the spam has originated. The Super Blacklist Service is equally powerful in blocking Asian language spam as it is in blocking North American and European spam.

A. How Does The Service Work?

The following diagram depicts how the core Service works.

Server A is the spammer email server.
Server B is the legitimate email server of an enterprise.
Server C is MailProve Super Blacklist server.



B. Features for Service Providers

MailProve's Super Blacklist Service includes features that are specifically designed to assist Service Providers:

- Evidence tracking and reporting to prove that individual users are spamming
- Early warning notification prior to blocking
- Automated "punishment" system for spammers
- Instant "unblock"
- Management and update modules
- Service Provider specific blacklists and whitelists

C. Platforms Supported

MailProve Super Blacklist Service supports all major platforms. If your platform is not indicated please contact us for further information: info@MailProve.com.

Sendmail	Qmail	Lotus Notes 6 or above	MS Exchange 2003
Ironport	Mirapoint	Brightmail	SurfControl
iMAIL	SOPHOS puremessage	CommuniGate Pro 3.5 or above	JSMail
Rblsmtpd	SLmail	Zmailer	Eudora Internet Mail Server 2.2
Smail 3.x	Obtuse smtpd	Stalker Internet Mail Server for Mac OS	Blackmail mail filter
Postfix	Tumbleweed MMS	exim	NTMail
N-PLEX	VOPmail	MailMarshal 3.0	

D. Hardware and Software Requirements

No additional hardware or software is required to use the Service. A simple configuration of your email server or MTA will connect to the Service.

E. "Super Blacklist" Features

MailProve's "Super Blacklist" offers much more than any standard blacklist. MailProve Super Blacklist servers are distributed in strategic locations around the Internet and specifically covering the Asia Pacific. We block spam on behalf of our customers wherever the spam has originated. The Super Blacklist Service is equally powerful in blocking Asian language spam as it is in blocking North American and European spam. The Super Blacklist servers are updated in real-time using an extensive array of techniques before deciding whether a particular message is a spam. This delivers real-time updates to combat new forms of spam that are being released every day by spammers. MailProve's systems and our team of spam engineers are constantly monitoring for new spammers and their techniques.

Other features include:

- Web based and windows based administration
- Management and reporting
- Whitelist import from outlook express, palm desktop, CSV and LDIF file
- Customer specific blacklist
- Spam detection in English and Asian languages
- Virus site blocking
- Instant unblocking

F. MailProve Infrastructure

MailProve is deploying a scalable, robust and resilient architecture throughout Asia Pacific. For a Service Provider it makes little sense to deploy their own blacklist and then spend valuable resources attempting to build features and keep it up-to-date. MailProve does all of this as well as ensuring it is designed for maximum performance and availability.

G. Support

MailProve is dedicated to supporting Enterprises and Service Providers in the Asia Pacific region. We block spam on behalf of our Asia Pacific customers wherever the spam has originated. Unlike other blacklist service providers that can take days to answer queries and do not provide phone support, we respond to customers usually immediately within Asia Pacific working hours and always within 40 hours from receiving the request. In addition, we offer self-service tools to customers so that they can perform various actions in real-time, e.g. become “unblocked” when meeting certain criteria.

Frequently Asked Questions (FAQ)

1. What is the response time of the MTA when using MailProve Super Blacklist?

The MTA which receives an email transmit request will use DNS to check the sender's IP address against the MailProve Super Blacklist. This check takes between ten millisecond and half a second (0.01 to 0.5 second) for every email transmission request received. Its deployment will save considerably more CPU time compared to filtering based anti-spam and anti-virus packages.

2. How up-to-date is MailProve's Super Blacklist?

Our global real-time Super Blacklist database is updated in real-time upon new spam and virus source detection. At the back-end of our Super Blacklist we have a number of spam and virus source detection routines running 24/7. These back-end routines upload identified spam and virus sources continuously in real-time. Companies can update their own blacklist and whitelist in real-time through using the MailProve tools "MailProve Minder".

Update frequency	For Enterprise	For ISP
Company level list	in real time	in real time
Global list	every 60 minutes	subject to contract

3. What is the accuracy of spam blocking?

Our empirical accuracy is that MailProve Super Blacklist blocks 95% of all spams.

4. How do we tackle Asia specific spam?

MailProve's back-end routines include algorithms to handle multi-byte languages such as simplified and traditional Chinese. In addition, our back-end routines operate across strategic locations distributed throughout Asia Pacific. We also provide multi-lingual service support to our customers.

5. Can an email administrator check the blocking status of their mail server or MTA?

Yes. They can make use of our system features to identify and resolve their out-bound email problems and improve their email service. An evidence system provides details for substantiating our Super Blacklist database.

6. Does MailProve “read” the content of my email?

No. MailProve’s Super Blacklist Service does not look at the contents of your mail.

7. How do we treat spammers?

Identified and continually repeating spammers are blocked from MailProve’s customers through our Super Blacklist Service.

For email administrators, they can check if their email server or MTA are inadvertently sending spam or viruses. They can apply for unblocking at any time as long as they are able to demonstrate they have cleaned up their spam or virus problem.

8. What is our anti-spam strategy?

Our intention is to help email administrators who are inadvertently sending spam, identify and resolve this problem. The rest of the solution is to block real spammers at source, thereby reducing our customers’ bandwidth and server costs as well as IT administration and end user time.

9. Can customers control their own blacklist and whitelist?

Yes. They can update their company level lists in real-time using the tools provided on MailProve’s Super Blacklist Service.

10. What happens when a large email system is blocked? Will that block all email from that location?

Yes and No. Unlike simple blacklists, MailProve’s Super Blacklist will warn the administrator beforehand to give them some time to address the problem and we will provide information to assist such as the IP address of the offending host. Once blocked, the administrator can apply for instant unblocking once the problem is demonstrably resolved. At any time a MailProve customer can override for themselves only the Super Blacklist by adding the offender their corporate whitelist. For consistent offenders, MailProve’s Super Blacklist includes a “punishment” system that will delay the reinstatement at increasing lengths of time.