MAILCHANNELS

Transparent Filtering

Analyze outgoing email traffic from your network to protect IP reputation

MailChannels Transparent Filtering blocks the delivery of spam from your dedicated and VPS hosting customers by transparently intercepting and blocking abusive email before it reaches the internet.

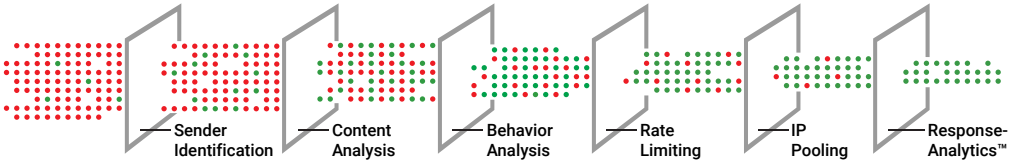
Eliminate email delivery challenges related to IP blacklisting

Analyze all outgoing SMTP traffic from your customer base without configuration changes. You can filter mail coming from servers, subscribers, scripts, and devices to achieve a blacklist-free network.

Scalable and fault tolerant

Transparent Filtering works in conjunction with your routers. The routers are configured using Policy Based Routing (PBR) to redirect outgoing port 25 traffic from the network to the MailChannels server.

With MailChannels, you can intercept the outgoing SMTP connections, analyze them, and forward them to the intended destination without modifying the source IP address. The mail will appear to be coming from each individual VPS or dedicated server, and your customers won't know that their mail is being filtered.



Transparent FIltering directs SMTP traffic through a series of analysis and filtering steps to identify the responsible sender, analyze message content, assess sender behavior, and then apply an appropriate rate limiting or blocking policy. Similar email can be grouped into pools for sending through IP addresses that are optimized for that type of traffic. Finally, responses from email receivers are automatically categorized to provide feedback that helps identify abuse and improve delivery.

Highlights:

- **Never worry about blacklisting** — let our team worry about the challenges of getting your email delivered
- **Speed up abuse detection** — identify compromised accounts so you can shut them down
- **Automate email abuse management** — identify compromised accounts so you can shut them down

MAILCHANNELS

Features

Transparent filtering

- Filter mail from servers, subscribers, scripts, and devices to reduce IP blacklisting
- Maintain the original source IP address and destination IP address
- Flexible SSL handling, enabling man-in-the-middle decyption of SMTP sessions where permitted by law

Compromised account detection

- Identify and shut down hacked accounts or malicious IP addresses in seconds, before they cause email issues
- Send automated notifications to system administrators

Policy Scripting

- Write expressive email policies in JavaScript
- Integrate with external LDAP, SQL, and Redis servers, query the DNS, and call out to web services using a fast, non-blocking API

Visibility

- Search email history with a powerful parametric log index
- Reduce time required to diagnose delivery problems and build evidence so you can shut down abusive users
- Ship logs to ElasticSearch, Splunk, or SIEM systems to merge outgoing email threat data with other security threat data

Scalability and clustering

- Handle up to 10,000 servers or 10 million end users on one server
- Real-time peer-to-peer clustering means no single point of failure
- Add/remove machines anytime

Reputation protection

- Use intelligent IP address allocation, apply rate limits, and monitor delivery rates

System requirements

The following configuration will process at least 30 million messages per hour and 10,000 SMTP connections per second:

- 8 x 64-bit Intel or AMD CPU cores
- 32 GB RAM
- 1 x 1000BASE-T NIC
- 500 GB SSD disk space

Designed for

- Dedicated/VPS Hosting Providers
- Cloud Service Providers
- Internet Service Providers

Unlimited

- Users / Admins
- Domains

24x7 support

Our support team is available 24 hours, 7 days a week to help with your service. Contact us for expert assistance in using your MailChannels solution to the fullest advantage.

Contact us

Email: sales@mailchannels.com
Toll free: +1 888 685 7488 (North America)
Tel: +1 604 685 7488 (International)