



The Maildistiller Email Filtering process

How it works

Maildistiller managed services are backed by a Telco quality infrastructure, spanning redundant Internet connections and hardware across multiple Data Centres which proactively protect your organisation from global threats on a local level.

External email by its very nature usually requires a message to be sent to or from your organisation. This can inevitably require the message to be relayed through several internet service providers before reaching its final destination, all of which are outside the control of the diligent security conscious organisation trying to protect its email servers and reputation.

What happens my email in technical terms?

Every time an external email is sent to a client of Maildistiller, the following process takes place:

- **The sender's MTA performs a lookup on the client's MX record, which will point to a Maildistiller MX host name**
- **Maildistiller's DNS Partner Verisign authoritative DNS servers are queried to determine the IP address of the host-name. VeriSign offer 100% availability of this service.**
- **If there are four different Clusters in a specific Silo, Verisign's DNS server will return one of four distinct IP addresses, each of which has a time to live (TTL) of 900 seconds**
- **The sender's MTA will initiate an SMTP connection directly to this IP address, and will continue to use this IP address until the 900 seconds expire.**

The sender's mail server, when trying to send email again to the same Maildistiller client (or any other Maildistiller client configured on the same Silo), will once again query the Verisign authoritative DNS servers to get another IP address for that silo. At any given moment, Verisign's authoritative DNS servers are responding to tens of thousands of requests for the IP addresses of our Silo's.

Each time Verisign's authoritative DNS servers are queried for a Silo's IP address, the server will give out the IP address of one of the Clusters in the Silo.

The next time that server gets a request for the same Silo, it will give out the next Cluster's IP address and continue to alternate until all four IP addresses in the cluster have been given out. The fifth request for the same cluster will cause the distributing load balancer server to loop back to the beginning, giving out the first IP address again. This is known as round-robin load balancing. The net effect is a random but equal distribution of the IP addresses of Clusters within a Silo.

When email is sent to a Maildistiller MX, it is handed off by the local router to a local load balancer (LB) which is configured to perform both NAT (Network Address Translation) and PAT (Port Address Translation).

The LBs act as a bridge between the external network facing the Internet and the internal network on which our secured mail servers reside. The LBs are tasked with deciding which mail server should scan each piece of mail. They are configured to decide when and how many emails to send to each mail server in the Silo. One of the components of this configuration is a 'Server Loading', which is a manually set value created when a new server is added to a tower.

Each mail server has a specific Load based on its processor/memory/disk utilisation specification. Most of the time, all servers are similarly loaded, as all servers in the Silo usually have the same hardware/software configuration. There are some exceptions, however, where we might add a more or less powerful server to a Silo. We would therefore adjust the configuration on the LB to account for this newly added server's capacity.



Maildistiller Email filtering process www.maildistiller.com

maildistiller™