Mail-SeCure™ Load Balancing

White Paper

Load balancing essentials

When building Mail-SeCure solutions, one of the ways to increase overall availability and performance is to provide redundancy for the SMTP sessions. Most email security solutions cannot provide such redundancy themselves and are dependent on third party solutions in order to achieve load balancing (image 1).

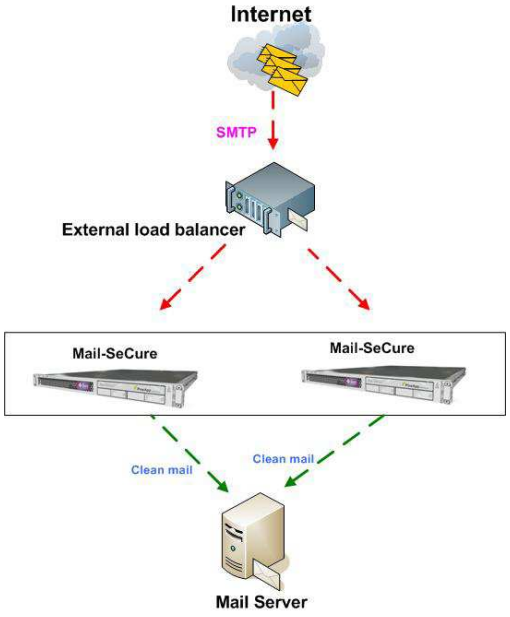


Image 1 – Load balancing achieved by external device

Unlike these solutions, Mail-SeCure features an embedded load balancer. This enables customers to achieve true load balancing capabilities without the need of the external device (image 2).

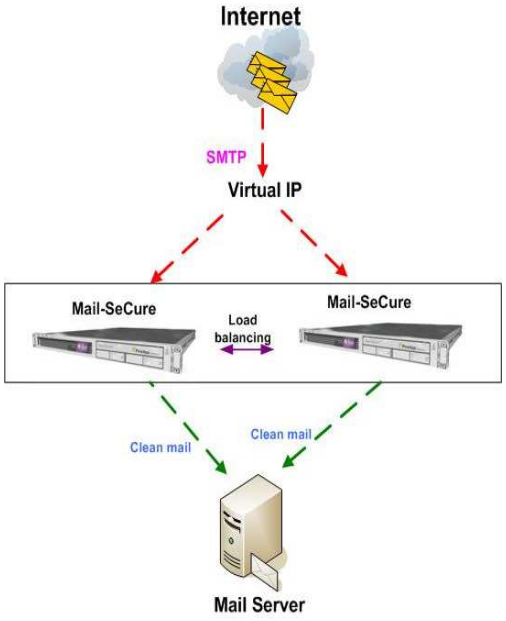


Image 2 – Load balancing achieved by internal engine

Mail-SeCure Load Balancing terminology

Master - The Mail-SeCure appliance that performs the routing function for the virtual IP at a given time. Only one master is active at a time.

Slave – Mail-SeCure appliances that are active but not in the Master state. Any number of slaves can exist. Slaves are ready to take on the role of Master if the current Master fails.

Virtual IP - An IP address that is not connected to a specific device or network interface card (NIC) on a device. SMTP packets are sent to the VIP address, but all packets travel through real network interfaces.

Active – Active – A status where all participant devices share some of the SMTP traffic load. It is possible to define weight for each device and control the amount of traffic that is distributed to each device.

Active - Passive – A status where only the Master device handles the traffic while the Slave waits in stand-by to automatically take over the Master role in case of failure.

Load Balancing in action

In the following example, the load balancing is demonstrated. Figure 3 illustrates a typical load balance configuration (active – active):

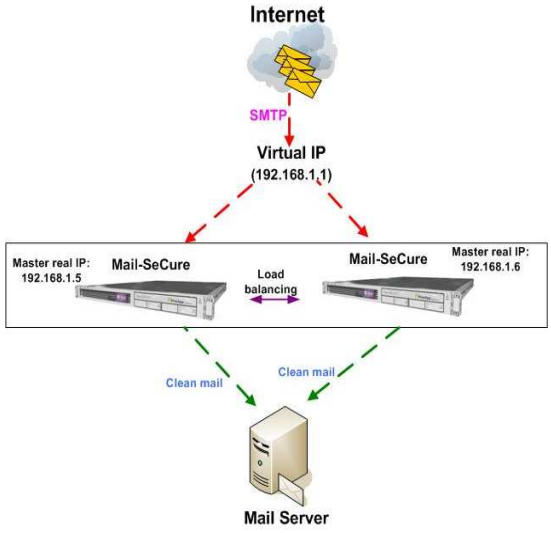


Image 3 – Typical load balancing configuration

When a Mail-SeCure is configured as a Master, it sends multicast packets advising the rest of the participants in the load balancing that it is the Master for that cluster. This serves two purposes:

1. If a device with a higher priority is started (for example the VIP owner), the new owner can force an election and take on the Master role.
2. The slaves expect this multicast. If an interval elapses without a packet being received, the appliances in the Slave state take action to elect a new Master (since in all likelihood the Master has failed).

In our example, we have configured Mail-SeCure Master priority to be 200 and Mail-SeCure's Slave priority to be 50. The Master will manage the Virtual IP and the multicasts.

Mail-SeCure failure

When the Master suffers a failure, after a short interval the Slave notices that no multicast packet has been received. It then transitions to the Master state, taking over the handling of the VIP and sends its own multicast packets.

The length of time that the Slave waits before making its state transition is called the "Master down interval". It is based on the length of time between Master updates (called the "advertisement interval") and a value called "skew time" which is calculated from the priority value.

Router restart

When the problem with the Master is resolved, and depending on its configuration, either of two situations occurs:

1. If the Master is configured to start as Master, it forces an election immediately by sending its first advertisement as Master. The Slave receives this advertisement and transitions to backup state.
2. If the Master is configured to start as backup it transitions from initialization to Backup state. Nothing happens until it receives an advertisement from the Slave. The Slave has a lower priority than the Master, so the Master starts an election by commencing its transition to Master state and sending an advertisement. When it receives this advertisement, The Slave transitions to backup state because the Master has higher priority.

Topologies

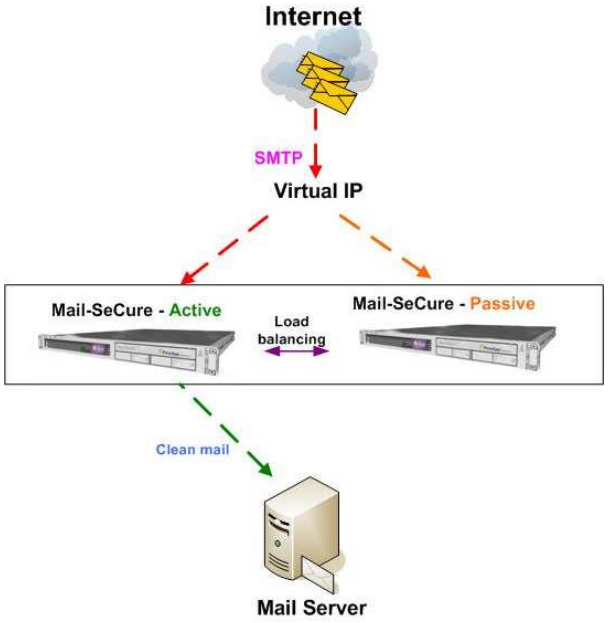
Active-Passive

A status where only the Master device handles the traffic while the Slave waits in stand-by to automatically take over the Master's role in case of failure. All logs and quarantine are stored on the active Master device at the given time.

Advantages:

1. Redundancy – if one Mail-SeCure faults, the passive system automatically takes over with no down time.
2. Management is done on the Active unit. If it faults, the management automatically transfers to the passive unit (which turns to active), Including daily reports and Black & White lists.

The disadvantage of this topology is that if a system faults, all the quarantine, logs and databases are not available. Also, it is not possible to add scanning abilities by adding additional devices.

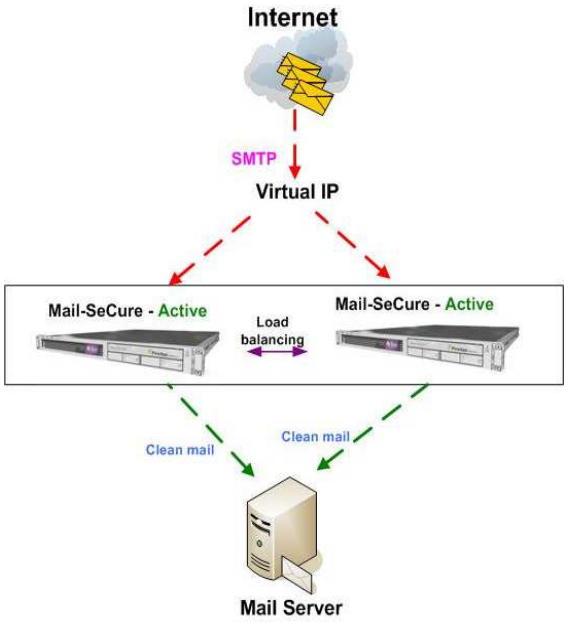


Active-Active

A status in which all participant devices share some of the SMTP traffic load. It is possible to define weight for each device and control the amount of traffic that is distributed to each device. It is possible to configure more than two devices in such topology.

Advantages:

1. Traffic is balanced between two devices, thus the capability to handle more traffic is doubled.
2. Ability to add more devices as the need of the organization grows
The disadvantage of this topology is that quarantine database and logs are distributed between all devices. However, this can be solved by the Scanner-Director topology (see Scanner-Director white paper).



Distributing configurations

PineApp's solution also offers to manage these clusters from the Master unit. Once changes, such as Black & White lists, rules or general configuration, are made on the Master the changes are distributed to the Slaves. The distribution is done manually.