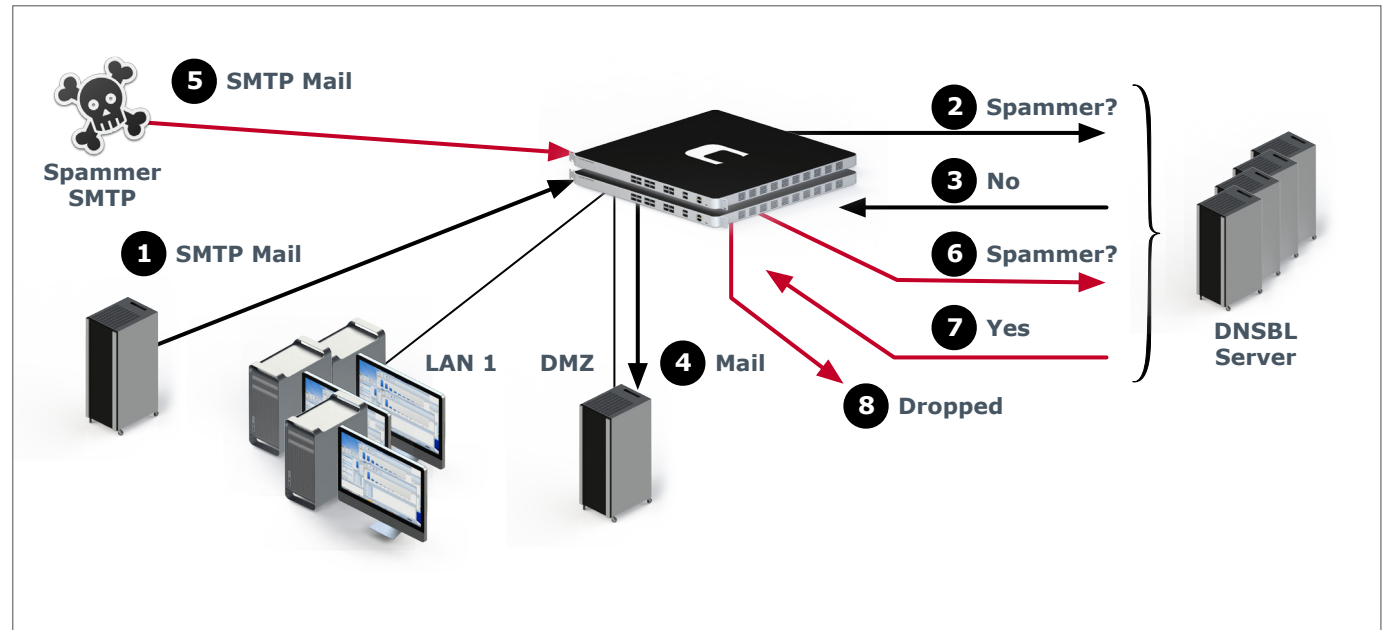**CLAVISTER ANTI-SPAM**

Anti-Spam

Clavister cOS Core-based products functions as an anti-spam solution scanning incoming traffic and collaborating with an array of configured DNS Blacklists. Blacklisted spammers will be dropped by the Clavister product.

Example

In this example, we have two SMTP servers that sends email. One labelled **Remote SMTP** that is not blacklisted and one labelled **Spammer SMTP** that is blacklisted. Each SMTP server sends email to users using a SMTP server residing on the DMZ labelled **SMTP Server**.

1. A remote SMTP server sends an email
2. The configured DNSBL servers are consulted – is the sender a known spammer
3. The replay is **No**, the sender is not a known spammer
4. The mail is forwarded to the SMTP server configured on the DMZ
5. The spammers SMTP server sends an email
6. Again, the DNSBL servers are consulted – is the sender a known spammer
7. In this case, the sender is a known spammer and the replay is therefore **Yes**
8. As a consequence, the mail is dropped by the Clavister units

RESOURCES

For more information about **Anti-Spam**, download the latest Clavister cOS Core Administration Guide from www.clavister.com/my-clavister/downloads/clavister-cos-core

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | www.clavister.com