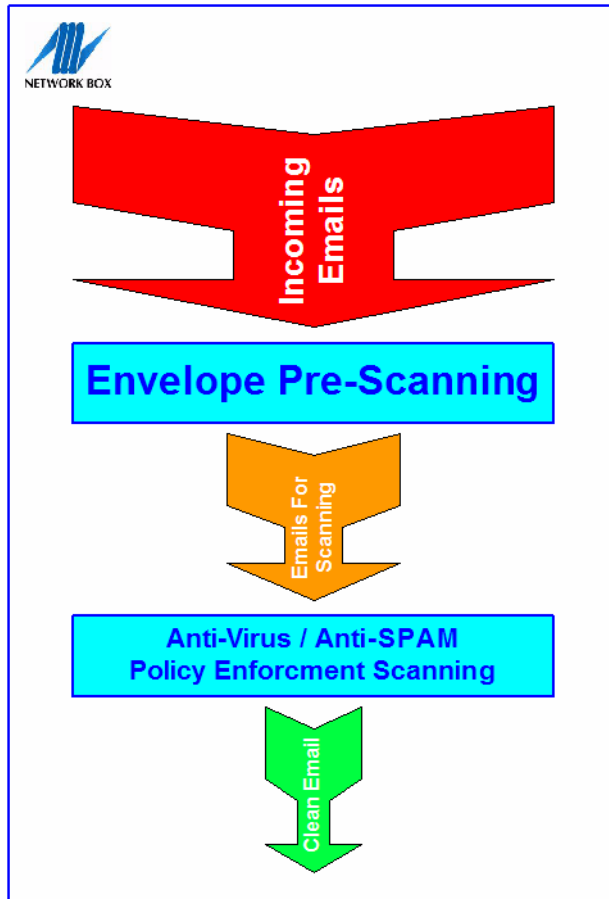


## Network Box Email Envelope Pre-Scan

### System Overview

Email envelope pre-scanning functionality, is a new technology which allows Network Box systems to make a very sound judgment on whether an email is from a spammer or not; without even needing to actually download and scan the email itself.



This can massively reduce unnecessary loading on Network Box units which are setup at the gateway. Pre-scanning email envelopes can also improve throughput, lower the stress on the Network Box hardware for increased long term reliability, and also free up valuable Internet bandwidth from being wasted.

There is a very significant upward trend in the number of spam emails being received by companies and organizations around the world. In some extreme cases, Network Box customers are finding that 98% of their emails are either viruses or spam. In large organizations, this can represent several hundred thousand unwanted spam emails arriving each day.

### Email Envelope Pre-Scanning Primary Advantages

"Pre-Scan Envelope" allows Network Box to pre-scan the email message envelope (module, sender's IP, sender's email address, recipient list) and return a result code, prior to actually accepting the message.

This has several key advantages. First of all, this can save very significant amounts of Internet bandwidth. If a message can be rejected BEFORE it is even downloaded, obviously there is no need to use any additional Internet bandwidth to download the actual email message.

Secondly, pre-scanning email envelopes saves both CPU and disk utilisation. Pre-scanning is very fast, and relatively simple. By pre-scanning, it is possible to reject emails known to be spam, without having to pass it through a full, very resource-intensive scan process.

This is especially true in the case of image based spams, which use graphics and photos instead of text, and therefore can only be safely blocked using state-of-the-art multi-pass OCR (Optical Character Recognition) technology. Doing OCR scanning requires significant CPU utilization.

Lastly, pre-scanning also allows Network Box systems to refuse "acceptance," meaning that the sender is then responsible for non-delivery notifications. This can very significantly reduce the email queues, and the overhead of NDR notification raising and delivery, on the Network Box system. Once again, larger organizations can suffer from non-delivery notification queues, which run into tens of thousands of outgoing emails. With pre-scanning, these queues can be massively reduced, and often eliminated altogether.

## Email Envelope Pre-Scanning Technical Bullet Points:

Currently, at envelope pre-scan, NBRS-3.0 provides for:

- Blacklisting of recipient email addresses (and domains).
- Blacklisting of sender email addresses (and domains).
- Blacklisting of sender IP addresses (and /8, /16, /24 ranges).
- Blacklisting of sender IP addresses by real-time blacklist lookup.
  - This technology is commonly called a “reputation system,” in anti-spam circles.
- Verification of sender email address (for local domains).
- Verification of recipient email addresses (for local domains).
  - Envelope Sender/Recipient Verification works at the entire email address (rather than domain) level. For example, say "acme.com" is our domain.
  - The box can already be told to accept email on behalf of "acme.com" for scanning and delivery, but what about individual users. As the box acts as a "backup MX", it can verify the domain, but it has no way of verifying the user part of the email address. Enter Envelope Sender/Recipient Verification. Under such a system, for each email address in a list of local domains, the box queries a remote server to verify that email address (including the user part of the address) and will only accept the email if the verification succeeds. In this way, the box can effectively combat non-existent email addresses (usually obtained by directory harvesting).
- Network Box uses a built-in system called PAM to do this verification. Currently there are “helpers” for:
  - Verification using LDAP (against an LDAP server).
  - Verification using SMTP (against an SMTP server with support for either VRFY or RCPT TO address verification).
- It is also important to note that with some sender/recipient verification systems, it is possible that information may be leaked, regarding which users exist and which don't. On Network Box systems, this is not an issue. Network Box systems accept the host, sender and recipient list, and then either accept, temporary fail, or permanently reject that entire set (with a suitable error message). Network Box systems, never reply that a particular email address is “invalid;” they merely reply that, "one or more of the sender's IP, address or recipients is not accepted".
- Frequently spammers forge the “sender” as well as the “recipient,” and they forge the sender as a local email addresses. An example of this would be a spam from "joe@acme.com" to "peter@acme.com". With “Network Box Envelope Sender Verification,” it is possible to verify the sender "joe@acme.com," to ensure it is valid.
- In extensive tests on live Network Box customer boxes, it has been clearly shown that as much as 60% of incoming spam email is cut out, by implementing sender/recipient verification. All this is done at the envelope level, before receipt of the message itself, saving huge amounts of resources and bandwidth.

***This feature is a standard part of NBRS-3.0, and in current released packages. All new Network Box S-M-E systems come with this new technology, as of Q4 2006.***