Blocking emails with a fake sender

iQ.Suite Tips & Tricks for Microsoft Exchange / SMTP

Distributors of spam use a variety of techniques to avoid anti-spam solutions. One of these is using SMTP sender addresses from the recipient's domain. iQ Suite Wall can easily detect and eliminate these emails:

Step by Step:

- The standards on which email is based allow scenarios in which information about the email sender or recipient can be faked. There are always two types of sender and recipient addresses.
- SMTP addresses: these are comparable with the address on a letter envelope and are used to deliver the email.
- Mail addresses: these are comparable with the address on letter paper and are shown in the email clients.
- This means that it is possible for you to receive an email which contains an internal sender address via SMTP, but which has nevertheless been sent from outside.
- An email that originates on your own email server contains a unique message ID. This, in turn, contains the name of your email server.
  For example:
- If an email is generated by the spam senders, it does not contain the name of your own server.
  This can be used as a criterion with which to block this kind of email.
- To do this, we will create a new Wall email address filtering job.
- This job first needs to process all the emails that are received by an internal sender via SMTP.
As another option, we choose Following Headers and Values on the Conditions tab.
Now we look for the emails which do not have your email server in the "Message-Id" field.
• These emails are then, for example, moved to an appropriate quarantine area.
• Important: this job only functions in this way from iQ.Suite 7.x on.