SecurityGateway

Account Verification Options

1. Users will be entered manually
– The administrator(s) will enter each user/ address manually to set them up in SecurityGateway.

2. SMTP "call forward" verification
– This verification source uses an SMTP session to determine whether email addresses exist on the mail server. If they do, they're automatically added to the database and the mail is accepted.
Note: When using SMTP "call" forward, at this time aliases will also count as users, so administrators should be aware of this when choosing a license size.

3. ActiveDirectory / Exchange
– SecurityGateway will query the AD/Exchange server to confirm the validity of any unknown email addresses. If they're found, they're automatically added and the full user list is pruned for any changes.
Note: When using ActiveDirectory, any aliases will be recognized as such and will not be counted as a "user" in terms of licensing.

4. MDaemon using Minger
– SecurityGateway will check with MDaemon's own Minger server to confirm the validity of any unknown email addresses.
Note: When using this verification method, any aliases will be recognized as such and will not be counted as a "user" in terms of licensing.

5.LDAP server
– SecurityGateway will query an LDAP database to confirm the validity of unknown local addresses.
Note: As with SMTP verification, at this time aliases will also count as users, so administrators should be aware of this when choosing a license size.