ESCOM Corporation, PO Box 626, Oakton, VA 22124

Spam Filtering with Active SMTP (ASMTP)

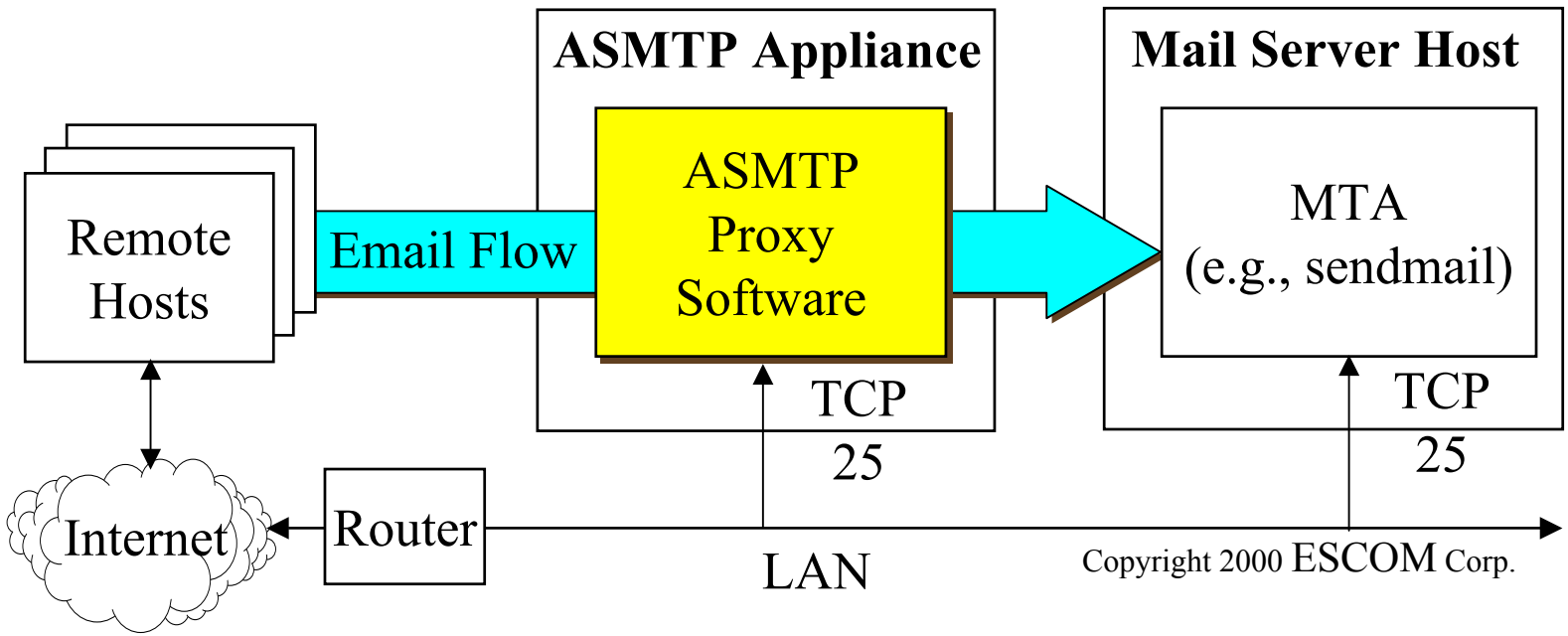
Albert Donaldson

al@escom.com
703-620-4823

http://www.escom.com

ASMTP Architecture

- ASMTP operates as MX host to handle incoming mail for one or more local domains
- Active Filtering, Content Filtering, Databases
- Forwards filtered mail to mail server



How ASMTP Blocks Spam

- Blacklists: local (IP, domain, addr) and RBL
- Eight Active Filters (underlined)
  - Remote host: DNS, HELO, relay*, client*
  - MAIL From: domain existence, domain match, existence of user address*
  - Header checks (Bcc, From envelope check, Received line analysis)
  - Exceptions may be quarantined or rejected
- Content Filtering - keyword and context
- virusrisk - blocking by file attachment type
- Web-based quarantine management

ESCOM

ASMTP Characteristics

- Most decisions during SMTP handshake
- Lightweight, buffer at a time processing
- Language-independent
- Local databases and local control
- Site Configurable
  - Trusted hosts/domains
  - Filtering modes and quarantine flags
  - Content, RCPTs, resource limits
- User Configurable
  - Per-recipient filtering configurations