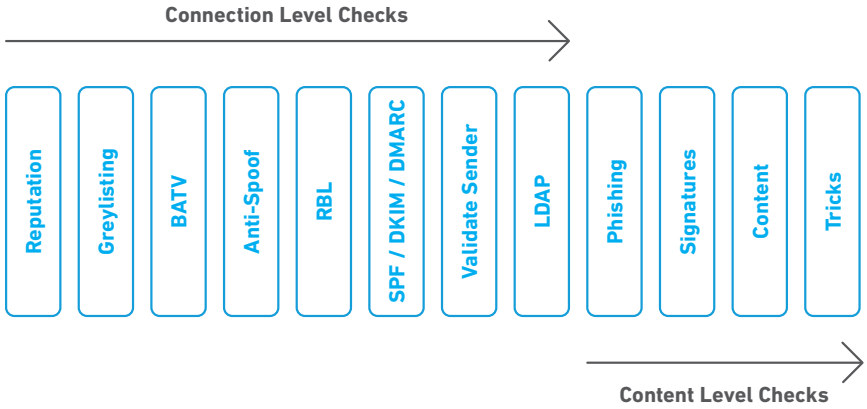
clearswift
RUAG Cyber Security

Anti-Spam

Inside the Clearswift SECURE Email Gateway there is a multi-layer Anti-Spam solution designed to deliver 99% detection with minimal false positives.



The Anti-Spam detects messages as being Spam, Phishing or Newsletters and allows system administrators to configure policies to either Block, Sanitize, Hold, Tag or Deliver.

- **Reputations** – Powered by TRUSTmanager. Every external message is checked against a real time database that contains the reputation of millions of IP addresses. If the reputation of senders IP is classed as BAD then the message can be dropped instantly
- **Greylisting** – If the sender's reputation is suspicious then we can initially reject the connection and request the sender to retry and deliver the message. This eliminates spam botnets and also reduces the amount of malware received by the system
- **BATV** – Detects non-delivery spam being received by the system. This is caused by people spoofing your internal email address and sending out spam mail, which if it causes a non-delivery report to be generated it will be sent to the spoofed sender
- **Anti-Spoof** – There are a number of algorithms built into the system to detect a spoofed message. This functionality is also aided by the use of SPF, DKIM and DMARC
- **RBL** – An integrated Real-time Block List, can be supplemented with multiple other RBLs, such as Spamhaus, Protected Sky, IBM, SORBS, etc. This is another system designed to look at the sender's IP address to check if it has been involved in spamming
- **Message Authentication Services** – The Gateway features 3 methods of message authentication
  - **SPF** – Checks sender IP against published list of sending IP's in DNS
  - **DKIM** – Receiver checks that if a DKIM header has been added by the sender it has been created using the same keypair as published in the sender's DNS record
  - **DMARC** – Uses SPF and / or DKIM results and performs additional checks to determine if message is valid
- **Validate Sender** – Checks to see if the sender's domain exists or not
- **LDAP** – Integrates with Active Directory and checks to see if the recipient does exist before accepting the message
- **Phishing** – Looks for the presence of URLs / attachments that indicate that this is a phishing message and not just bulk spam or Newsletter. Allows Phishing mail to be separated from "normal spam"
- **Signatures** – Identifies message that are sent in bulk
- **Content** – Looks for offensive content
- **Tricks** – looks for message formatted or sent to bypass anti-spam rules