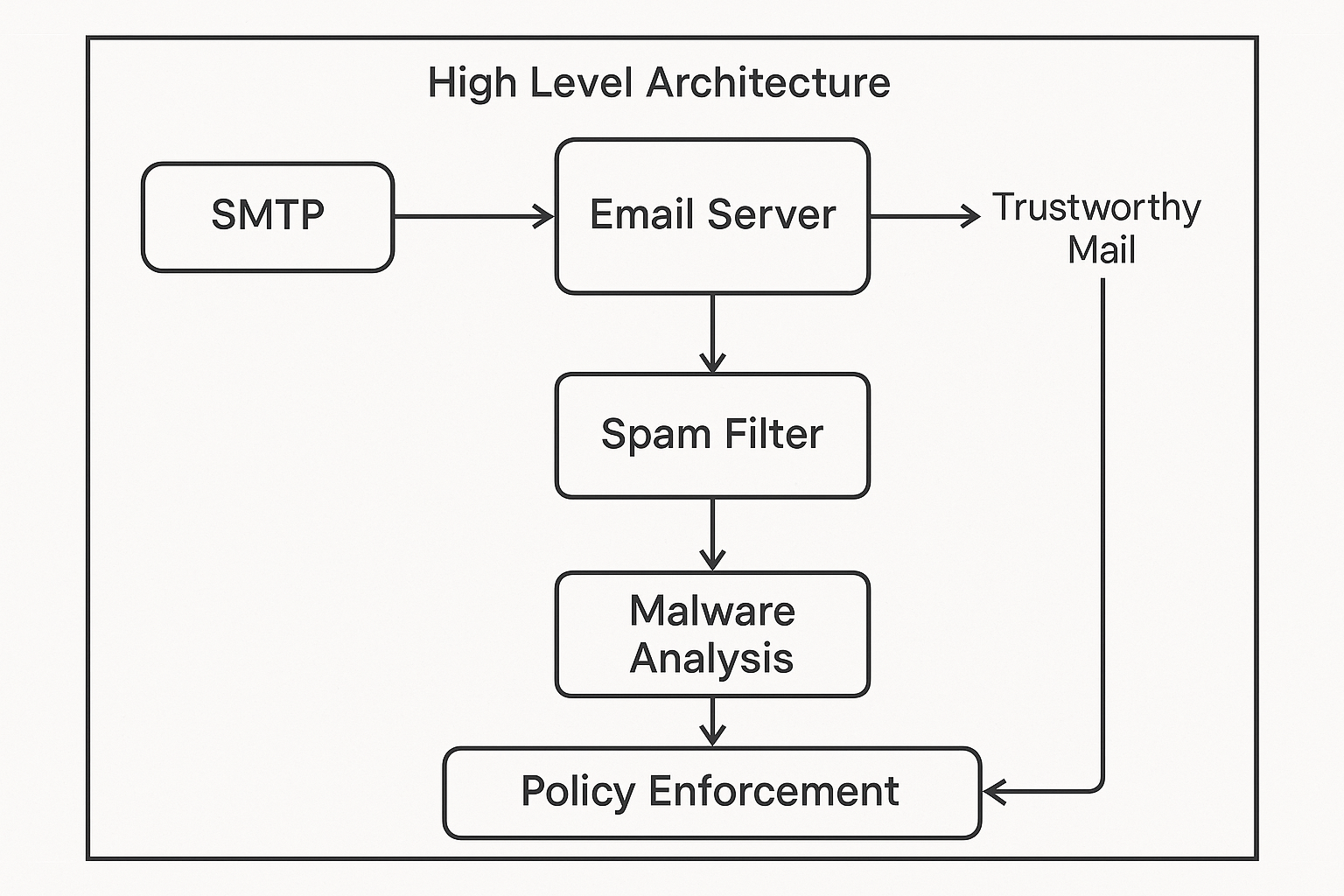
Secure SMTP Email Infrastructure – Charter/Spectrum

# Overview

This document outlines the high-level architecture and full infrastructure of a secure email scanning system for spam, malware, and untrustworthy content within the Charter/Spectrum ecosystem. The goal is to provide a secure, scalable, and policy-driven mail platform that ensures subscriber safety.

# High-Level Architecture Diagram

The diagram below shows the key components involved in mail processing:



# Infrastructure Components and Roles

## SMTP Gateway Layer

Accept mail traffic over port 25/587, enforce TLS, and block known bad sources.

* - SMTP Proxy (Postfix, Exim, Sendmail, etc.)
* - TLS Certificates (Let's Encrypt, Entrust)
* - Rate Limiter / Throttler
* - DNSBL/Spamhaus Integration

## Inbound Email Server

Receives email after handshake and routes to spam filters or user mailbox.

* - MTA (Postfix, Exim), MDA (Dovecot, Cyrus)
* - SPF / DKIM / DMARC validation
* - SMTP AUTH / SASL

## Spam Filtering Cluster

Assigns spam score and determines if mail should be quarantined or passed on.

* - SpamAssassin / Rspamd
* - ClamAV / Sophos AV
* - Bayesian Classifier, Greylisting, Heuristics

## Malware & Attachment Analysis Sandbox

Detonates or analyzes attachments to detect malware or exploits.

* - Cuckoo Sandbox, YARA Rules
* - ClamAV, Bitdefender, Fortinet
* - File-type whitelisting

## Policy Enforcement Engine

Handles blocking, quarantine, user notification, and routing.

* - Custom Lua/Go/Python Policy Logic
* - Quarantine System (Amavis, MailScanner)
* - Rate/Geo/Behavior-Based Filters

## User Mailbox Backend

Stores and serves filtered mail to authenticated users.

* - IMAP/POP3 Server (Dovecot)
* - Maildir/PostgreSQL
* - Webmail (Roundcube, SOGo), OAuth2

## Monitoring & Threat Intelligence

Correlates threats, visualizes patterns, and raises alerts.

* - SIEM (Splunk, Elastic, QRadar), MISP Feeds
* - Syslog Forwarding, Prometheus/Grafana

# Vulnerabilities and Mitigation Strategies

|  |  |  |
| --- | --- | --- |
| Threat Vector | Description | Mitigation |
| Spoofed Emails | Emails appearing from legitimate Charter/Spectrum domains | SPF, DKIM, DMARC |
| Malware Attachments | Executable/macro content | AV engines, Cuckoo sandbox, File-type blocks |
| Phishing Links | Redirects to malicious sites | URL Rewriting, Safe Browsing APIs |
| Rate-Based Attacks | Mass SMTP connections | Greylisting, Connection Throttling |
| Zero-Day Exploits | Undetected malware | Dynamic sandboxing, Heuristics, Threat Feeds |
| Weak SMTP Auth | Credential brute-force | TLS, OAuth2, 2FA, GeoIP |
| Insider Threats | Employees misusing access | SIEM, UEBA, Audit Logs |
| DNS Hijacking | Rerouting mail delivery | DNSSEC, MTA-STS |

# Recommended Deployment Matrix

|  |  |
| --- | --- |
| Host/Pod Role | Services |
| smtp-gateway-1 | Postfix, TLS proxy, DNSBL |
| filter-node-[1..N] | SpamAssassin, Rspamd, ClamAV, Policy Engine |
| sandbox-node-[1..N] | Cuckoo Sandbox, AV engines, YARA |
| mailbox-backend | Dovecot, PostgreSQL, IMAP/POP3 |
| webmail-ui | Roundcube, OAuth2 connector |
| monitoring-node | Prometheus, Grafana, Syslog |
| siem-node | Splunk, Elastic, MISP connector |
| admin-portal | Policy editor, Quarantine UI |