HIN GATEWAY – STARGATE

High-Level Technical & Operational Overview

1. Infrastructure Prerequisites

Server Requirements

- Dedicated Linux server or virtual machine
- Recommended sizing (the VM size may be smaller depending on message throughput):
  - 4 CPU cores
  - 8 GB RAM
  - 30 GB persistent storage
- Internet connectivity required for image retrieval, certificate services, logging, and mail routing

Supported Operating Systems

- RHEL 8, 9, 10 compatible distributions (e.g. Alma Linux, Rocky Linux, CentOS Stream)
- Ubuntu 22 or 24
- Debian 11, 12 or 13

Deployment Model

- Docker-based deployment using Docker Compose
- All services run containerized on a single host (scalable by design)

2. Network & Firewall Requirements

Inbound Connectivity (must be allowed)

- TCP 25 – SMTP (receiving mail from external mail servers)
- TCP+UDP 19818 – WireGuard (encrypted agent-to-agent communication)

Outbound Connectivity (must be allowed)

- TCP 443 – HTTPS access to external platform services (image registry, CA, sealer, issuer, verifier, logging)
- TCP 25 – Outbound mail delivery to destination mail servers (via MX lookup)

DNS Requirements

- Full DNS resolution must be available
- Required DNS record types:
  - MX (mail routing)
  - SPF (sender allowlisting)

    - A / AAAA records
- DNS is actively used for mail routing, relay configuration, and security checks

3. Required Configuration Inputs

Prior to deployment, the following customer-specific information is required:

Mail & Identity

- Mail domain to be handled by the HIN Gateway instance
- Public IP address or publicly reachable URL of the HIN Gateway instance
- Organization and country details for S/MIME certificate issuance
- DNS names to be included in certificates

WireGuard (MGW-to-MGW Communication)

- Exchange of public keys and endpoints with peer MGWs
- Firewall allowance for UDP WireGuard traffic

4. Core Components (High-Level)

The HIN Gateway deployment includes the following logical components:

- **Postfix Relay**
  Handles SMTP ingress and egress and integrates with MXEngine
- **MXEngine**
  Performs mail processing such as signing, encryption, sealing, and policy-based routing
- **Policy Engine**
  Uses OPA/Rego policies stored in a database and optionally synchronized from Git
- **IDAgent (WireGuard)**
  Establishes secure tunnels between all HIN Gateway instances for secure message delivery
- **Vault**
  Secure storage for encryption keys, certificates, and secrets
- **PostgreSQL**
  Stores mail metadata, policies, agent configuration, and system state
- **MinIO (Object Storage)**
  Stores messages and attachments securely
- **Monitoring & Logging**
  Prometheus-compatible metrics and centralized log shipping

5. Operational Considerations

Startup & Restart Behavior

- Vault automatically seals on container restart as a security measure
- Controlled startup procedure is required to unseal Vault
- All data is persisted across restarts via Docker volumes

Backups

- Automated daily backups are configured by default
- Backups include:
  - Databases
  - Vault keys and secrets
  - Configuration files
  - Certificates
- Backup responsibility and retention policy should be agreed with the customer

Policy Management

- Mail routing and delivery logic is governed by policies
- Policies can be centrally managed via Git-based synchronization
- Changes are applied safely

6. Dependencies

External Dependencies

- Container image registry
- Certificate authority services
- Remote sealing services
- Issuer and verifier services
- Central logging and monitoring endpoints

Internal Dependencies

- DNS and network availability
- Correct firewall configuration
- WireGuard peer coordination