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)

Port	Protocol	Direction	Purpose
25	TCP	Inbound	SMTP — receiving mail from external mail servers
8084	TCP	Inbound	HTTP seal-callback from the HIN sealer service. Plain HTTP is intentional — the seal payload itself is already encrypted, so no additional TLS is required on this listener.
19818	TCP + UDP	Inbound	WireGuard — encrypted agent-to-agent communication

Outbound Connectivity (must be allowed)

Port	Protocol	Direction	Purpose
443	TCP	Outbound	HTTPS access to platform services: container image registry, S/MIME CA, remote sealer, issuer service, log shipping
4433	TCP	Outbound	HTTPS access to the verifier service
19818	TCP + UDP	Outbound	WireGuard — peer tunnel to the HIN CA and any directly connected peer agents. The same port must be open inbound and outbound, and on both TCP and UDP, even if only TCP transport mode is used initially.
25	TCP	Outbound	Outbound mail delivery to destination mail servers (via MX lookup)
53	TCP + UDP	Outbound	DNS lookups (MX, SPF, A/AAAA, PTR)

Note: ports 8081–8083, 9000/9001, 8200, 5432, 1587, 10026 and the 2113–2116 metrics range are exposed locally on the host for diagnostics and monitoring. They are not intended for inbound traffic from the public internet and should remain blocked at the perimeter.

DNS Requirements

- Full DNS resolution must be available
- Required DNS record types:
  - MX (mail routing)
  - SPF (sender allowlisting)
  - A / AAAA records
  - PTR (reverse DNS for outbound mail reputation, recommended)
- 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 WireGuard traffic on TCP and UDP, inbound and outbound (port 19818 by default)

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