



# AMG

AIR-GAP MAIL GATEWAY



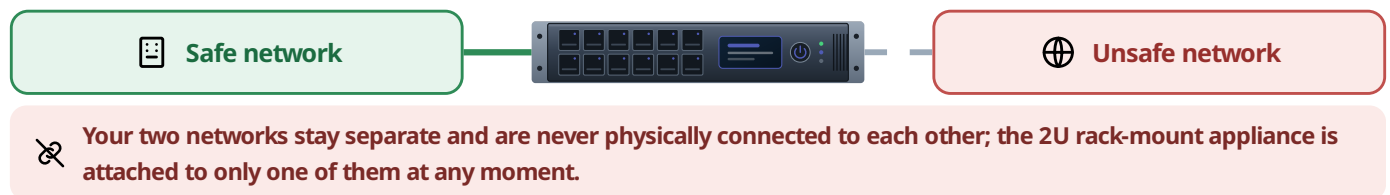
2U RACK-MOUNT APPLIANCE

## Security and isolation: a relay that leaves nothing open

Peers, transport security, secrets, Postfix hardening and the privacy of content, on an appliance that keeps the two networks physically apart.

**For:** Security specialists**In this catalog:** Transport security, a full stop on any failure, the privacy of content, and events for your SIEM<https://www.bardin.tech/en/bardingate-amg/>

AMG is an email entry point, so it asks the hardest security question first: who may connect to me? The answer is two IP addresses and no more. The rest of the design keeps that answer true for the life of the appliance.



### Physical isolation



A physical switch inside the appliance joins one of the two networks at a time and fully disconnects the first before joining the other. At every start everything is disconnected first, and the state is proved by the switch's own feedback.

### Trusted start



UEFI Secure Boot, boot measured into a TPM 2.0 chip and a read-only system verified block by block.

### An encrypted queue



The persistent queue sits on the appliance's encrypted data volume (LUKS2 and AES-256-XTS), and RAID tolerates one disk failure.

### A hardened, independent Postfix



Rootless Podman, a read-only root, AppArmor, seccomp, no extra system privileges and resource ceilings; a process apart from the rest of the appliance's software.

### Cryptography



The console speaks TLS 1.3 only; signatures are ECDSA over P-256 with SHA-256; passwords use Argon2id. MD5, SHA-1, 3DES and RC4 are never used.

## Peers and transport security

| Control                   | How it works                                                                                                                                                             |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP allowlist</b>       | Only a direct connection from the two configured addresses is admitted. Each is an IPv4 or IPv6 address written as numbers; a hostname in the address field is rejected. |
| <b>No DNS, no MX</b>      | Connections always go straight to that IP address. The hostname is only the peer's identity and the name expected in its certificate.                                    |
| <b>TLS mode</b>           | REQUIRED is the default and validates the peer's certificate without exception. OPPORTUNISTIC and OFF need an explicit warning and an audited apply.                     |
| <b>mTLS and SMTP AUTH</b> | Optional and set per side; certificates, keys and passwords are held only as references to the secret store.                                                             |
| <b>Direction</b>          | From the peer's IP only; altering a message cannot change it.                                                                                                            |

### Secrets live nowhere else

Private keys and passwords never enter the configuration file, logs, database, diagnostics or SIEM. The file carries only their addresses in the secret store.

## Any failure stops the flow

- An unknown peer, the same IP on both sides, an invalid TLS identity, a missing required secret, an ambiguous direction and malformed configuration are all refused.
- A configuration is first checked ( `postfix check` ), activates only when healthy and otherwise rolls back.

## The privacy of content

- Bodies, attachments and subjects never appear in logs, metrics, database metadata or SIEM events.
- In the SIEM, sender and recipient addresses default to a stable keyed pseudonym with a masked display. Full and omitted are explicit alternatives, and full carries a warning and an audit record.
- The pseudonym is a keyed HMAC with a purpose-separated key in the secret store; plain unsalted hashing is prohibited, and rotating the key starts a new generation.

## The security posture at a glance

|                          |                                           |                                 |                                                  |
|--------------------------|-------------------------------------------|---------------------------------|--------------------------------------------------|
| <b>Peers</b>             | Exactly two, with fixed and different IPs | <b>TLS</b>                      | Required by default, with certificate validation |
| <b>Open relay</b>        | Never                                     | <b>DNS and MX</b>               | No lookups at relay time                         |
| <b>Secrets</b>           | References only in configuration          | <b>Message content</b>          | Unchanged and in no log or event                 |
| <b>Postfix execution</b> | Rootless, read-only, AppArmor and seccomp | <b>Joining the two networks</b> | Never; no physical connection between them       |

## Identity and access

- **The appliance is the only authority.** The browser, imported files and everything else bring claims; none can grant authority.
- **The default is deny.** Roles carry an explicit scope, and a permission not written is a refusal.
- **Password, and the password again.** High-risk actions (roles, security policy, licence and update import, time correction, recovery, configuration import) ask for it again.
- **No back door.** There is no vendor master password, hidden account, email reset or unaudited bypass. Recovering the last administrator is a physical procedure at the unit.
- **SSH reaches only a restricted support account.** It returns reports, logs and status and nothing more; root has no SSH login and there is no routine shell or direct database access.

## Events for your SIEM

| Event          | When it is raised                                                           |
|----------------|-----------------------------------------------------------------------------|
| MAIL_ACCEPTED  | A message was durably accepted                                              |
| MAIL_DELIVERED | The opposite MTA accepted it                                                |
| MAIL_DEFERRED  | Delivery failed temporarily, with a stable reason and the next attempt time |
| MAIL_FAILED    | A permanent failure or expiry; a DSN was issued                             |

Delivery to the SIEM is one-way, and a SIEM fault never blocks SMTP. All security and audit events are exported by default as well.

### ✦ Security without extra work

All these controls are the appliance's defaults and are on as delivered; you only enter the two peers' addresses and your certificates.

## A relay that talks to two addresses only, with valid certificates only, and never judges content.

More about this product

### CATALOG 1

Product overview

### CATALOG 2

Mail flow and queue

### CATALOG 4

Operations and integration

For advice, a demonstration and contact details:

<https://www.bardin.tech/en/bardingate-amg/>



Specifications may change without notice.