Netframe

SECURITY

Security Hardening Guide for Netframe Deployments

A high-level security configuration overview covering network isolation, role-based access control, audit logging, and compliance considerations

May 2026 · Version 1.0

Contents

Overview

Netframe ships as a hardened, single-image deployment built on Debian stable with the management plane provided by Netframe Manager. The default configuration is conservative: minimal exposed surface, modern transport security, and strong authentication primitives. This document covers the security posture decisions an operator should make on top of those defaults.

It is intentionally broad rather than deep. The goal is to make sure that, on the day a security review arrives, the right controls are in place and the operator can explain what they are and why. For deployments with formal compliance requirements (ISO 27001, SOC 2, IRAP, PCI-DSS), the principles below are the foundation; the specifics will be shaped by the auditor's framework.

Network isolation

The Netframe management plane should not share a network with workload traffic. This is the single largest reduction in attack surface available.

Three network segments are typical:

- **Management network.** Reaches Netframe Manager, the Core hosts' management interfaces, and the storage appliance management interfaces. Accessible only from operator workstations and bastion hosts. Not routed to the public internet.
- **Cluster network.** Carries HA heartbeat, live migration traffic, and inter-host coordination. Hosts only. No VM traffic.
- **Workload network.** Carries VM traffic on whatever VLANs and subnets the workloads require. The boundary between workloads and the management plane is enforced at the network layer, not just at the host firewall.

Storage traffic typically rides its own dedicated network for performance reasons; the security boundary follows the same principle as the cluster network: hosts only, not exposed to VMs.

Open vSwitch on each Core host enforces the VLAN trunking that keeps these segments separate. Misconfiguring a VLAN tag is the most common way the boundary gets accidentally crossed; validation should be a step in every change procedure that touches network configuration.

Identity and access control

Netframe Manager supports local accounts and Microsoft Active Directory for authentication today. Additional identity providers (LDAP, SAML 2.0, OpenID Connect) are on the roadmap. For any production deployment with an existing AD estate, the recommendation is to integrate with AD rather than maintain local accounts. The benefits are familiar: centralised onboarding and offboarding, audit trail of authentications, and access removal that takes effect within minutes of a personnel change rather than waiting for someone to remember to remove a local account.

On top of authentication, Netframe Manager supports role-based access control with both built-in and custom roles. The principle to apply is least privilege: most users in most organisations need read access to most of the platform and write access to a small subset of it.

Three role patterns are common:

- **Operator.** Day-to-day VM lifecycle: power, console, snapshot, backup-restore. No cluster or platform configuration changes.
- **Administrator.** Operator capabilities plus cluster configuration: host management, network and storage configuration, role assignment.
- **Auditor.** Read-only access to all resources, including audit logs. No write or execute capabilities.

Service accounts (for automation, monitoring, CI/CD) should use scoped API keys or short-lived service-account credentials rather than reusing operator or administrator accounts. Each service account should have the minimum role required for its function and should be reviewed quarterly.

Audit logging

State-changing actions performed through Netframe Manager are recorded for operational and audit purposes. Netframe Core hosts also support standard syslog forwarding, so platform-level events can be sent to your existing log aggregation or SIEM infrastructure.

The reason to forward off-box is straightforward: if the only copy of an operational log lives on the appliance, an attacker who compromises that appliance can also tamper with the record of the compromise. Off-box archival is what allows post-incident forensics.

Retention should match the longest applicable regulatory requirement. Seven years is a defensible default for most enterprise contexts.

Transport security

Every network-exposed Netframe endpoint uses TLS 1.3 by default. The management UI, the REST API, the inter-host control plane, and webhook deliveries are all TLS-encrypted.

Certificate management is the recurring operational task. Two options:

- **Internal CA.** The recommended option for management-plane traffic. Issue certificates from your existing internal CA, distribute the CA root to operator workstations and automation systems, and use the CA's existing rotation process.
- **Public CA via ACME.** Supported for the Manager UI if it is exposed to corporate networks where distributing an internal CA is awkward. Not recommended for inter-host or storage traffic.

Whatever the certificate source, automated rotation is what keeps the platform secure between security reviews. Manual rotation is the most common source of TLS-related outages.

Encryption at rest

Encryption at rest for VM disks is the responsibility of the underlying storage layer. Most enterprise NFS appliances support transparent encryption against physical disk theft and are the right place to enforce data-at-rest encryption in a Netframe environment. Choose the appliance and key-management posture that matches your threat model and compliance framework.

Patching and lifecycle

The single-image deployment model means Netframe updates ship as a complete, signed image rather than a stream of individual packages. Two implications for security.

First, the patching process is simpler: download the updated image, apply via the documented update procedure, reboot. There is no package manager state to drift across a fleet, no firmware compatibility matrix to validate against a kernel version, no agent that may or may not be at the right level.

Second, the cadence is predictable. Security patches are bundled into image updates and ship on a published schedule. Critical patches ship out-of-band when required. The security team can plan against a known cadence rather than reacting to a continuous package stream.

The hardened image profile disables unnecessary services and ports by default. Operators should resist the urge to install additional packages directly on the Core host; if functionality is needed, the right path is usually a VM or a sidecar on the management network, not modification of the hardened image.

Compliance considerations

The controls above map to the common control families in ISO 27001, SOC 2, IRAP, and similar frameworks:

- **Access control:** Local + Active Directory RBAC, least privilege, regular access review.
- **Audit and accountability:** Manager audit log, syslog forwarding from Core hosts, defined off-box retention.
- **System and communications protection:** TLS 1.3 by default, network segmentation, encryption at rest at the storage layer.
- **Configuration management:** hardened image, predictable patch cadence, change control on cluster configuration.
- **Identification and authentication:** AD integration, scoped service accounts via the REST API.

For specific compliance frameworks, the operational specifics will vary. Neon Dynamics can provide control mappings against a named framework on request.

Recommended checklist

A short checklist to validate the deployment against. None of these are platform features; they are operator decisions that must be made and documented.

- Management network is segmented from workload traffic and not exposed to the internet.
- Cluster and storage networks are physically or virtually separated from workload traffic.
- Identity is integrated with Active Directory. Local Manager accounts exist only as break-glass.
- RBAC roles defined per the principle of least privilege. Service accounts use scoped credentials.
- Syslog forwarding from Core hosts is configured to an off-box destination.
- TLS certificates are issued from a managed source with rotation scheduled.
- Encryption at rest is enforced at the storage layer where required.
- Patch cadence is defined, scheduled, and tested in a non-production environment first.
- Quarterly access review removes accounts and credentials that are no longer required.

Next steps

If you are preparing for a security review, the practical next steps are:

1. Walk the checklist above against your current deployment.
2. Capture the control mappings against the framework you are being assessed against.
3. Contact Neon Dynamics if you need control documentation for specific frameworks. For IRAP, ISO 27001, and SOC 2, common control mappings are available.

A hardened default is the starting point; documented operational discipline is what makes the platform pass audit consistently.