Air Gap Server

An **air gap server** is a computer system physically isolated from unsecured networks, including the Internet, to protect critical data from remote cyberattacks. This isolation—combined with full disk encryption and strict physical access controls—provides defense-in-depth against ransomware, unauthorized access, and compromised source systems. The system typically remains powered off except during scheduled backup operations, with data transferred via encrypted removable media ("sneakernet"). This approach is particularly valuable for long-term backup storage where the reduced attack surface and offline state dramatically limit exposure to both network-based and physical threats, making it an essential component of a comprehensive disaster recovery and business continuity strategy.

Documentation

- Air Gap Server Concepts — Security principles, encryption strategies, and implementation best practices
- Sneakernet Implementation — Production deployment guide for automated ZFS replication via encrypted transport media

Quick Links

- Encryption Strategy — GELI, split-keys, and transport encryption
- Example Workflow — Typical backup cycle walkthrough
- Installation Guide — Getting started with sneakernet
- Key Management — Generating and rotating encryption keys

External Resources

- FreeBSD GELI Encryption
- FreeBSD ZFS Handbook
- NIST Storage Encryption Guide
- Sneakernet Source Repository (SVN)