

Introduction

I've set up a Synology NAS (Network Attached Storage) system in my home to create a secure and private cloud for storing personal files and data. This system is connected to a Ubiquiti network, ensuring high-speed internet and robust security. The NAS is organized into different segments, or VLANs, that separate various types of devices, like trusted computers, smart home gadgets, and experimental setups, each with strict rules to keep everything safe. I use advanced security measures like firewalls, encryption, and frequent snapshots to protect against data breaches, ransomware, and physical damage. Regular backups are made to an external drive, so even in case of a total system failure, data can be recovered.

For accessing files, I've implemented a role-based system where each user has their own secure space, and specific groups can access shared folders. Two-factor authentication and strong passwords add extra layers of security. The system is also designed with redundancy, using technology that duplicates data across multiple drives, ensuring no data is lost if one drive fails. External access to the system is managed through Synology's secure QuickConnect service, making it easy and safe to connect from anywhere.

I'm using the DS923+ model, which currently holds 12 TB of storage space utilizing Seagate NAS Hard Drives. This document covers my setup and the best practices I followed to ensure a smooth user experience in the most secure way possible. This infrastructure setup is designed using **GDPR**, **ISO/IEC 27001** and **SOC 2 Type II** standards.

Content of Document:

1. Network Security
 - a. Network Setup
 - b. Firewall and Security Setup
 2. Synology Setup
 - c. User and Group Policy
 - d. Folder and File Permissions
 - e. Security and Firewall
 - f. QuickConnect
 3. Redundancy and Backup
 - g. Redundancy
 - h. Snapshots
 - i. Backups
-

Revision #1

Created 2026-03-09 17:13:39 UTC by lumxux

Updated 2026-03-09 17:14:13 UTC by lumxux