# Synology Setup

## Network Security

### Network Setup

This NAS is located at my private residence behind a Ubiquiti Router, in a separate VLAN. Ubiquiti, an American tech company, specializes in home and enterprise network and security systems and infrastructure. Their system provides robust network performance and security, employing a least privilege framework to ensure high speeds and firewall integrity.

The Synology NAS is connected to a Ubiquiti switch that offers OSI layer 2 and 3 security.

### Firewall and Security Setup

The security and firewall are configured using Ubiquiti's system and router capabilities. The Synology NAS resides in its own VLAN, which can only be accessed by my local computer and laptop via OpenVPN, utilizing Access Control. Other devices are placed in separate designated VLANs (trusted wired devices, trusted wireless devices, IoT devices, and homelab) with strict firewall rules governing specific communication protocols.

For example, trusted devices can communicate with IoT devices, but not the other way around. The IoT network is isolated and cannot see any other devices in the house.

Additionally, I utilize Ubiquiti IDS and IPS (Intrusion Detection System and Intrusion Prevention System) at the highest level, with an OSI layer 7 Next Gen Firewall. Furthermore, network access is restricted to only US, Canada, Australia, and select European IP addresses (websites and devices).

Lastly, no VLANs are set up with port forwarding, while the homelab and Synology VLANs use Cloudflare Tunnel for specific traffic tunneling.

## Synology Setup

In addition to a tight network setup, Synology is configured with security and redundancy in mind, ensuring your data stays secure in the unlikely event of a breach, ransomware attack, or physical/weather damage.

### User and Group Policy

All files and folders are secured using a combination of Role-Based and Attribute-Based Access Control.

- **Role-Based Access Control (RBAC)**: Access is configured based on roles, such as administrator or user. Rights are granted implicitly instead of explicitly. Each user is assigned a role and placed in a group with a specific access level.
- **Attribute-Based Access Control (ABAC)**: Access is configured based on parameters such as location and the application used to access files.

Permissions are group-based, assigned according to users' needs. For example, I can access the folders named "Mainers" and "LLLiB," but Margaret can only access the "Mainers" folder. Each user has their own folder for personal files and photos. All groups can access files only through Synology apps on their phones or iPads or by using personalized links.

The default administrator and guest accounts are disabled at all times. A specific account with administrator rights is created and can access Synology NAS through the DSM (DiskStation Manager) management tool from a local personal computer (ACL rule using MAC address). To log in to the admin account, I need to use a specific device, a 30-character password, push notification from my phone, and a passkey (Yubikey with touch).
Each user is required to use a 16-character password with two-factor authentication set up with the Synology push notification app. Synology apps like Drive and Photo only need to be signed in once.

Only user login activity is logged, meaning I don’t collect any usage activity, only who logged in when and from where. This is reviewed only in case of abnormal activity or when you report suspicious activity. This information is only available to me and is not shared or accessible by any non-administrator user or Synology itself.

img?tid=%22RVJnFOeBYcTrgnw_3kf-3Cy9ACkENwq_Ecz2qgxeck1UC53bcAtyyQLPMclnkD33ZxdFq8G
img?tid=%22RVJnFOeBYcTrgnw_3kf-3Cy9ACkENwq_Ecz2qgxeck1UC53bcAtyyQLPMclnkD33ZxdFq8G

## Folder and File Permissions

Each user has their own personal folder called "home" or "My Drive" for storing documents. Each user also has a personal folder called "photos" for storing their personalized photos.
These folders are ONLY available to individual users and cannot be accessed by others. The administrator can access these folders with the user's permission, by approving access through the Synology secure sign-in app (the same app used for two-factor authentication). This is only required if the user needs me to see or edit a file that cannot be shared with my non-admin account. For backups or recovering old file versions, this access is not required.

### Shared Folders

Each group is assigned a shared folder, with some groups accessing more than one. These folders can be accessed via the Synology Drive app or website.
In addition to file folders, there's one Shared Photo Folder called "Photo." It can be accessed via the Synology Drive app or website but is recommended to be accessed via the Synology Photo app or website. Access to this folder is set at the group permission level, and all groups have access.
Some subfolders, like "Carpenters," are only available to users in the "Mainers" group.

## Security and Firewall

File and folder security is controlled by group access, but for additional security, I have set up an Anti-Virus system that performs continuous scans. Additionally, the device and all applications are updated regularly with the latest patches.
In addition to the network-level firewall, there is a native firewall on Synology for more secure access to files and folders.
These rules allow only specific access to the administrative management portal from designated IP addresses, and access to only necessary applications. For example, you can see your files through the Synology Drive app or website, but you can't use FTP or SSH to access the machine and view the files.
No ports are forwarded, and external access is available through Synology QuickConnect. Denial of Service protection is enabled, allowing only 5 password attempts per IP address before being blocked.

img?tid=%22RVJnFOeBYcTrgnw_3kf-3Cy9ACkENwq_Ecz2qgxeck1UC53bcAtyyQLPMclnkD33ZxdFq8G

## QuickConnect

Synology QuickConnect allows you to access your NAS from outside my local network. It creates specialized secure Tunnel allowing you access to my network in order to access Synology Drive. However you are only accessing the drive itself that is isolated from the rest of the network.

Only devices with a randomly generated 20-character QuickConnect ID can connect.
Synology creates special web links with this ID for you to connect to Synology Drive or Photos in your browser. To make it more user-friendly and secure the link, this web link is converted to a personal link using my own domain, utilizing Cloudflare DNS and Tunnel.

Synology Drive Admin Console to see which user is connecting from what device and IP address, making sure that only trusted devices can access Synology device.

---

Revision #1
Created 2026-03-09 17:14:24 UTC by lumxux
Updated 2026-03-09 17:16:24 UTC by lumxux