Mobile Access to NAS via PMG's Stealth Remote Access Solution

Q: Can the PMG allow me to access my NAS remotely without exposing it to the internet or the vendor's tracking?

A: Yes. The PMG creates a private, secure tunnel that eliminates internet exposure and vendor reliance.

The PMG does not require you to configure your NAS to be directly accessible from the internet. It ensures you maintain zero exposure in three ways:

1. **Zero Internet Exposure:** Your router is left alone; no ports are opened.
2. **Zero Vendor Reliance:** You never use the NAS vendor's cloud-based services or registration.
3. **Local Access Only:** Once the OpenVPN Connect client is active with your PMG profile, your remote device is securely placed *inside* your private LAN. You simply access the NAS using its private IP address, exactly as if you were physically at home.

For step-by-step instructions on setting up this local access, please refer to the NAS Instruction guide on our website.

Q: I have a NAS on my private LAN. How do I access it remotely from my Endpoint device using the Primes Lab PMG?

A: Accessing your NAS with the PMG is simple and requires absolutely no configuration or port forwarding on your router.

The PMG creates a secure tunnel that makes your remote endpoint device appear as if it is physically inside your home network.

Setup and First Connection (on your LAN)

1. **Find Your NAS IP:** Note the local IP address of your NAS (e.g., 192.168.1.100).
2. **Install OpenVPN:** Install the OpenVPN Connect app on your Endpoint device.
3. **Configure the PMG profile:** Import the OpenVPN client profile obtained from your **activate.primes.com** subscription into the OpenVPN Connect app.
4. **Map Network Drive:** While your endpoint device is still on the same private LAN, map a network drive to your NAS using its local IP address (e.g., \\192.168.1.100).

Remote Access (Off-site)

1. **Disconnect:** Disconnect your Endpoint device from your private LAN.
2. **Connect to Internet:** Connect your endpoint device to the internet from any remote location (e.g., a coffee shop, another Wi-Fi network, or cellular data).
3. **Activate VPN:** Launch the OpenVPN Connect app and connect using your PMG profile.
4. **Access:** After the VPN connects, open a standard SMB client—File Explorer (Windows), Finder (macOS), or Files (iOS/Android)—and use your previously mapped network share to reach the NAS as if you were on your home network.
5. **Use third-party tools:** You can use any backup, restore, and sync apps/utilities in place of your NAS vendor's cloud app.

Q: I currently rely on DDNS and port forwarding to access my NAS. When I take my Win11 machine on the road, what's the secure way to reach the NAS without opening ports?

A: The Primes Lab PMG allows you to securely access your NAS directly, eliminating the need to expose your Win11 host or your NAS to the internet.

Your current setup is a common but complex workaround. The PMG replaces this host-based entry point with a secure VPN tunnel, allowing your laptop and mobile devices to connect directly to your private network from anywhere.

PMG's Recommended Solution

1. **Remove Host Exposure:** Disable the DDNS and port forwarding rules for your Windows 11 host machine on your router.
2. **Clean the NAS:** Remove any port forwarding and disable any cloud services or registration with your NAS vendor. (You won't need the vendor's cloud apps anymore.)
3. **Set up the Tunnel:** Install the OpenVPN Connect app on your endpoint device, iPhone, and iPad, and load the PMG client profile credentials.
4. **Map the Drive:** Connect your endpoint device to your local LAN and map a network drive to your NAS using its private IP address (e.g., \\192.168.1.100). Crucially, do not use port numbers.

How Remote Access Works Now

Once configured, the PMG ensures all your devices can access the NAS privately:

- **From Anywhere:** Simply open the OpenVPN Connect app on your endpoint device, iPhone, or iPad and connect. The secure VPN tunnel makes your device appear to be on your local network, allowing the mapped drive (or mobile file app) to connect instantly and securely.
- **Locally:** Your devices access the NAS normally when connected to your home Wi-Fi.

This shift replaces a complicated, exposed Win11 host setup with a simple, secure, direct-to-NAS VPN connection.

Q: Why shouldn't I completely trust my NAS vendors?

A: If you want complete privacy, you shouldn't rely on *any* third party, including your NAS vendor.

A vendor's cloud-based remote access turns your NAS vendor into an unnecessary relay that can monitor everything. To ensure your access is truly private and secure, you must take control of the connection path. The only way to do this is with a self-hosted VPN.

NAS Vendor Access (High Risk)	Self-Hosted VPN Access (Low Risk)
You Register: Identity is known and logged by the vendor.	**No Registration**: Identity remains private.
Vendor Controls Path: They are the relay and can track when you connect.	**Private Tunnel**: You control the path directly to your LAN.
Vendor Tracks Actions: They can monitor what files you access through their app.	**Local Access**: You use standard, private Samba utilities.

Q: Why should I use a self-hosted solution like Primes Lab PMG instead of registering directly with the NAS vendor (e.g., Synology, QNAP)?

A: For superior privacy and security based on the Zero Trust principle.

While most people worry about hackers, the greater, often overlooked security issue is the potential for NAS vendors themselves to log or track your NAS access. When you register and use their cloud-based services, the vendor becomes a data relay with total control over your connection.

This vendor relay can record your activity because they control all three security points:

1. **Identity**: You register, giving them your email and personal information.
2. **Path**: You connect through their cloud servers, giving them the transmission path.
3. **Action**: You use their app, allowing them to track your file access.

The PMG/VPN Advantage: Breaking the Chain

A self-hosted VPN solution, like the one offered by the PMG, completely bypasses this risk:

Privacy Factor	**Vendor Cloud Access**	**Self-Hosted VPN (PMG)**
Registration	Required; they log your personal identity.	None; your identity is private.
Transmission Path	Controlled and monitored by the vendor.	Private tunnel; vendor is bypassed.
File Access	Via vendor app; activity can be logged.	Via Samba/local apps; activity remains private.

To achieve true privacy, treat your NAS purely as hardware. Never use the vendor's cloud apps or registration. Instead, use a self-hosted VPN and standard local file utilities (like File Explorer or the Files app) for all access.

Q: If the Zero Trust principle means I shouldn't trust NAS vendors, why should I trust Primes Lab?

A: The goal isn't to replace one company you trust with another; it's to create a system that requires you to trust no one.

Under the Zero Trust model, you are right not to trust any single entity—not Synology, QNAP, or even Primes Lab. The problem with vendor-specific cloud access is that the NAS vendor controls the entire access chain: your identity (through registration), the data

pathway, and your activity. This concentration of control makes logging and tracking simple.

The most secure approach is a **self-hosted VPN**, which breaks that tracking chain, making your access private and secure. However, setting up a home VPN is often too technical for the vast majority of users.

The **Primes Lab PMG** is a **zero-configuration, zero-registration, and zero-tracking** solution that makes this highly private, self-hosted VPN model accessible to everyone. If you already know how to set up your own VPN, you don't need our product—but for the rest of us, Primes Lab delivers top-tier privacy without technical headaches.