**Q: What is Primes Lab PMG solution in a nutshell?**

A: It is a smart VPN.

**Q: Is it VPN 2.0?**

A: No.

**Q: Are all VPNs created equal?**

A: No. Not all VPNs are created equal.

A **commercial VPN service** does task no more than allowing the user to bypass the geo-fence to browse/access some of the Internet functions that were once blocked. It does not allow the user to go to the private LAN that the user has the right to visit.

A **corporate VPN** allows the user to visit the resources at the corporate LAN, including the PC or storage servers that the user is authorized to access. It requires a fixed WAN IP domain of a corporation.

For a corporate VPN to work at the user's private LAN with a dynamic WAN IP address, it requires additional work:

1. A dedicated VPN server including the hardware and software deployed at home LAN
2. An IT Technical staff to setup the VPN server
3. A skill to setup the home router with proper port mapping
4. To register a dynamic DNS for the dynamic WAN IP address at home

Without a networking expert to complete the above tasks, it is virtually impossible to deploy the corporate-grade VPN server at home on LAN.

It is why even if it is obvious that VPN can address privacy/security issues for consumers, it has not been widely deployed at home so far.

**Q: How is Primes Lab smart VPN different from other VPN?**

A: Prime Lab smart VPN solution is to be deployed at the user's private LAN:

1. It can do what a commercial VPN can do by allowing the user to access internet via the network PMG is connected to.
2. It can do what a corporate VPN can do by allowing the user to access PC and storage servers at home.

In addition, Primes Lab solution can do what a corporate VPN cannot do:

1. Without requiring a fixed WAN IP address or domain at home. A dynamic WAN IP address is sufficient.

2. Without requiring a VPN server at home
3. Without requiring an IT staff to set up the VPN server
4. Without requiring setup of the home router port mapping
5. Without requiring registration of a dynamic DNS for the dynamic WAN IP address
6. It is plug-n-play and can be setup in less than five minutes
7. After successful setup, it allows the user to be able to access all Matter compatible smart home appliances privately and securely on the private LAN.
8. It further allows private and secure chat among authorized users accessing the solution through the LAN-mode app on their endpoints which is not trackable or monitorable by any other third parties, including the ecosystem provider or the app developer.

**Q: Why has the solution not been thought of until now?**

A: The problem that Primes Lab intended to solve is an exceedingly difficult one. Many other solutions that tried to address privacy/security usually focused their attention on encryption. But it did not solve the fundamental man in the middle problem arising from the ecosystem provider as the go-between. Primes Lab's approach took a completely different route. Our aim was to eliminate the go-between problem altogether. Our approach brought the user privately and securely back to the private LAN through the VPN. Once the user was there, all issues to do with privacy and security were natively resolved. Of course, Primes Lab must clear all the hurdles in applying the corporate-grade VPN onto the private LAN as mentioned above. At the end of the day, the complexity was translated to how to make a plug-n-play smart VPN setup at the average user's home. Primes Lab's Smart VPN™ technology builds its defensibility and moats against other copycats, be them large or small. It took 20+ patents and years of effort to achieve where we are today.

**Q: Why now is the right time to deploy Primes Lab solution?**

A: There are several reasons:

1. After Apple announced the App Tracking Transparency policy in April 2021, 75% of the users have since opted out, bringing up global privacy/security awareness.
2. Matter standard started unifying the smart home appliances protocols after version 1.0 deployed in October 2022. It mandates that all Matter compatible smart home appliances run only on LAN mode.
3. Matter standard levels on the playing field in the smart home appliances market. But it does not address the tracking and monitoring problems arising from the go-between cloud-server scenario that has been plaguing the consumer's confidence in privacy and security from day one.
4. While Matter standard clears one of the biggest hurdles in the smart home appliances market by unifying the protocols, Primes Lab's smart VPN solution completes the last piece of the puzzle by offering private and secure access to all digital assets on the home LAN from anywhere in the cloud.

**Q: What is PMG, and why do I need it**

A: PMG provides a secure VPN service that requires no configuration effort to the public. If you want to remotely securely access data/devices in your private LAN, PMG provides such a service without any IT expertise (it is configuration free) which is often associated with the high cost and time that the corporate world employs.

**Q: What is the primary use case for PMG?**

A: The primary use case for PMG is to have a secure path to data/digital resources stored in your private LAN from the internet. When you travel outside your physical premises, you still enjoy private and secure access to digital resources in your private LAN with client devices.

While it is possible to use PMG for IP Masking, it is not the primary function for PMG. PMG allows secured inward traffic to your local network rather than to access the internet.

**Q: What are the factors that impact the performance of PMG's VPN access.**

A: Since PMG builds VPN tunnel. The following factors have a real impact on the PMG experience.

a. The bandwidth (speed) of your internet access at the private LAN location and the bandwidth/internet speed that your remote device that accesses the local private LAN. The slower speed between the two defines the actual speed.
b. VPN tunnel is built by encrypting and decrypting the data at the end devices. So, the power of CPU on the end devices-your phone or your tablet, or your laptop etc., impacts your data accessing experience.
c. A VPN tunnel is also built on underlying IP addresses. As mobile devices travel across different cell towers, the IP address will change. That means the existing VPN tunnel will break and needs to be rebuilt each time the underlying IP address changes. This will seriously impact on user experience. The underlying IP addresses change frequently as is the case when your end device travels through different cell towers.

d. Another impact arises from the VPN tunnel data path. If you will use PMG to access internet (probably for the purpose of IP address masking) while you are on the road, the data travels from your end device through the internet to your home router to your PMG, then it is routed out through your router to the web site on the internet. Compare this data path to a direct traffic path from your remote device to the internet website directly; lots of extra miles are added when you access the internet through the PMG. So, if you plan to access the internet from your device, it is best to bypass PMG unless you want to do it for other purposes.

   Also, in this case, if you download a big file, say 800MB, from the internet, the download speed will be much faster without going through PMG.

**Q: How is PMG different from VPN services that I use to access my company's network?**

A: PMG provides the same level of security and anonymity to the prying eyes when remotely accessing data stored in a private network, just like a corporate VPN service does. But with PMG, you don't need an IT Department to deploy it. Simply connect PMG to your private router's ethernet port, power it up and it is ready to provide VPN service.

**Q: How is PMG different from other commercially available VPN services like SurfShark, NORD, ExpressVPN and so on?**

A: PMG allows secure connection/tunnel into your private network remotely so you can access data in your private network. Commercial VPN services such as SurfShark, Nord, ExpressVPN provide secure anonymous access to the internet from your private network or from your device while you are on the road.

So, the simple difference is that PMG brings secure traffic into your private LAN, while commercial VPN services bring your traffic out to the internet.

**Q: How do I know if my PMG is working**

A: Simply connect your PMG to your home router with an Ethernet cable, power it up, and wait 5 minutes for it to be ready. On your phone or laptop, switch the connection to data instead of Wi-Fi (or connect to a public Wi-Fi hotspot). Run the OpenVPN Connect client software configured with the provided OpenVPN profile to make the connection. You will see the green button on the app when a connection is successfully made. Then open a browser on your device, type in the IP address for your home/private router in the navigation bar, and if you see your router information page, you know the PMG is working.

**Q: My connection through PMG gets interrupted from time to time when I roam, what happened?**

A: Your device's IP is part of a VPN tunnel. When you travel, your device's IP address can change when you travel through different cell towers. As the address changes, the VPN tunnel is first broken, then rebuilt. And it takes time to rebuild. As you travel across different cell towers, you may experience access interruption as the VPN tunnel/service goes through a rebuild process due to IP address changes.

**Q: It takes a long time to download large files from the internet when I connect through PMG.**

A: VPN tunnel is encrypted. There is overhead for this encryption process in terms of processing power. In a mobile device, if you are trying to download a large file, say a 800 MB file, from the internet through the PMG, the data encryption/decryption process incurs additional time in addition to the extra traffic. Also, your download request has to go from your mobile device to your private network where the PMG sits, then go back out to the internet site for the download and the data will go to your home, encrypted by the PMG then back to the internet to your device for decryption before processing.

In contrast, a direct connection without encryption between your device and the internet will require much less time.

Downloading large files from the internet going through the PMG (your private LAN) from a remote device is not a recommended use case for the PMG.

**Q: I plan to use Remote Desktop over my PMG connection, what is the process?**

A: To use Remote Desktop, you need to configure both the target Host and the client to turn on the service; in addition, since PMG is based on level 3 network protocol, knowledge

of host/resource IP address is needed. Please refer to specific Remote Desktop connection instruction (link to the instruction file here).

**Q: I have a NAS; can I use PMG to access my NAS without exposing the NAS to the internet or to the NAS vendors?**

A: Yes, you can access your NAS remotely using PMG even if your NAS is not configured to be accessible through the internet. The only requirement is that your client has been properly configured to access your NAS using IP address of your NAS in the private LAN. In this case, simply load up the OpenVPN Connect client with your profile, then access the NAS the way you did when your device was physically on the LAN.

**Q: I have a NAS in my private LAN, how to access my NAS remotely via PMG?**

A: Please note, the following steps require NO port forwarding and NO configuration on your router. Your router should be left alone, no configuration is needed on it.

Note your NAS IP (xxx.yyy.zzz.100) address in the local private LAN.

Connect your Windows laptop device to the same private LAN, run OpenVPN Connect app and configure it with the OpenVPN client profile that comes with your PMG then close it.

From the Windows laptop, map a network drive to your NAS (use IP address of your NAS not its name), in this case, it is xxx.yyy.zzz.100. Access the NAS through the Mapped network drive.

Disconnect your laptop from your private LAN. Reconnect it to the internet from a different LAN (through cell data service or in an internet cafe). Run the OpenVPN Connect app, then you can access the NAS just like if you are in your own private LAN.

**Access NAS using mobile devices (iOS/Android)**

**Q: I access my NAS with a DDNS+RDP+port forwarding setup on my Win11 host machine. I need to take that Win11 machine with me when I travel in order to access my NAS. Then there won't be any entry point left at home unless I set up my NAS with DDNS+RDP+ port forwarding.**

A: Prime Lab suggests the following:

1) Restructure your network resources.

2) Remove port forwarding setting for your NAS from the router.

3) Load the client credentials to OpenVPN Connect app to your laptop.

4) Connect your laptop to your local LAN and map your NAS, say, at 10.0.0.31, a private LAN IP as a network drive to your laptop. Don't use port number at all.

5) You should be able to access the NAS at your private LAN both when you are on the LAN or from anywhere on the Internet through PMG using the properly configured OpenVPN Connect app.

6) All your iPhone/iPad should be able to access the NAS from home LAN or from anywhere on the Internet through PMG with the properly configured OpenVPN Connect app.

7) Disable your registration to your NAS vendor and disable the cloud-mode app from the NAS vendor. As a matter of fact, from now on, you don't need your vendor's NAS app any more, after enabling PMG.

Q: Can I do site-to-site VPN with PMG

A: Yes, Site-to-site VPN can be set up easily with PMG. You do need separate PMG for each LAN that you want to connect.