Mobile Access to site-to-site VPN via PMG's Stealth Remote Access Solution

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

A: **Yes—PMG makes site-to-site VPN easy.** You'll need **one PMG per LAN**.

Setup

- Place a **PMG at Site-A** and another **PMG at Site-B**.
- Generate each site's **OpenVPN client profile (.ovpn)** and install **both** profiles on your endpoints (Device-A, Device-B).

How access works

- **When Device-A is on Site-A and runs Site-B's OpenVPN profile:** Device-A reaches all devices on **Subnet-A (native LAN)** and, via the PMG tunnel, devices on **Subnet-B (virtual LAN)**.
- **When Device-B is on Site-B and runs Site-A's OpenVPN profile:** Device-B reaches all devices on **Subnet-B (native LAN)** and, via the PMG tunnel, devices on **Subnet-A (virtual LAN)**.
- **Off-site:** Either endpoint device can connect to **Site-A or Site-B** by selecting the corresponding profile. **One VPN at a time** per endpoint.

Tip: Use **different subnet ranges** at each site (e.g., 192.168.10.0/24 and 192.168.20.0/24) to avoid routing conflicts.

Q: I have similar LAN addresses at both sites (e.g., \\192.168.10.100). Will there be IP conflicts once I connect the 2nd network with the PMG?

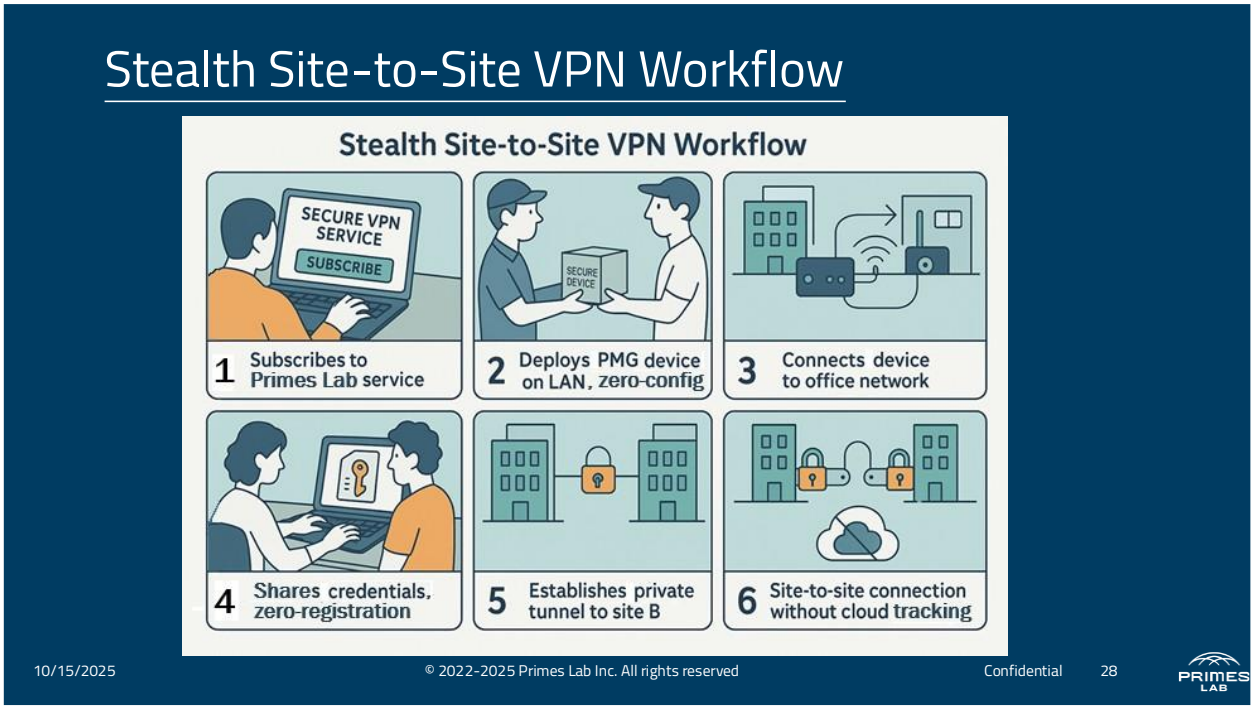
A: Using two PMGs on networks with the same IP range is fine if you access each independently.

But when you try to reach LAN-A from LAN-B through the target LAN's PMG, you'll hit routing conflicts due to overlapping subnets.

Recommendation: assign each LAN a different subnet (e.g., 192.168.10.0/24 and 192.168.20.0/24) to avoid IP conflicts and routing issues.

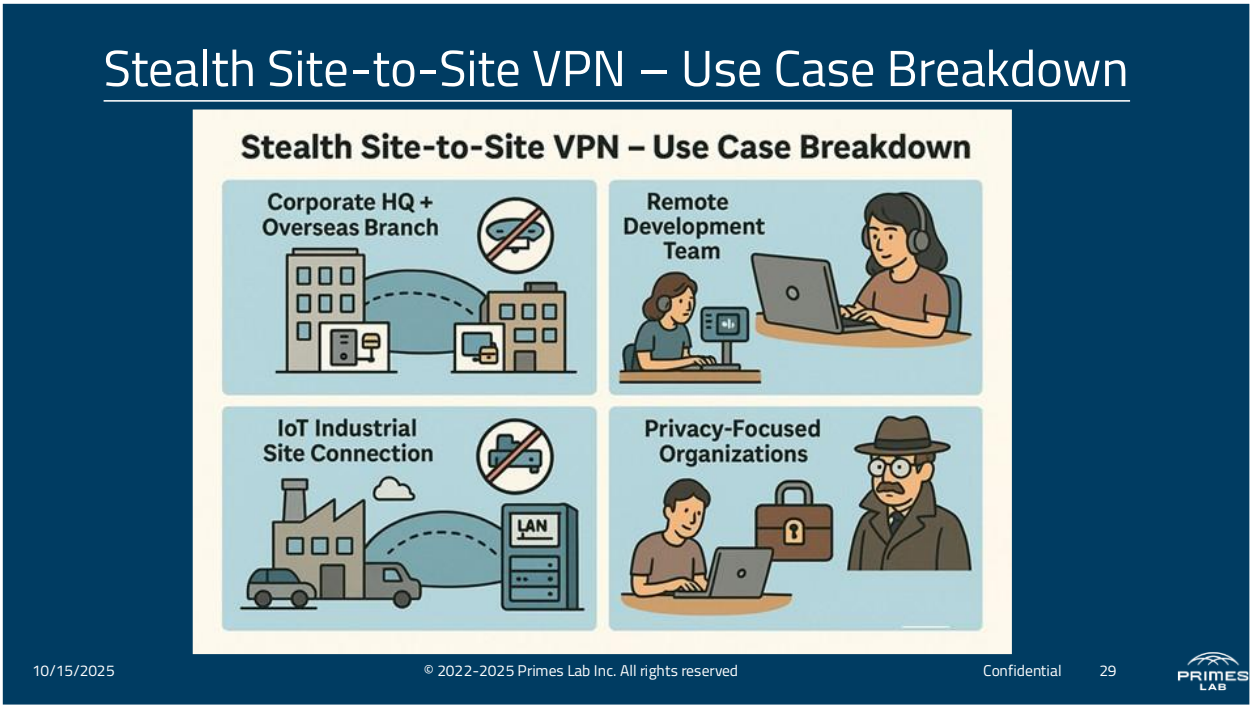
Q: What is the site-to-site VPN workflow?

A:



Q: What is the site-to-site VPN use case breakdown?

A:



Q: What is the example of a site-to-site VPN application?

A: Attached is a site-to-site VPN diagram for Bitcoin private-key backups. You can ignore the NAS at each site—they're only used for on-demand access to the virtual cold storage holding the keys.