VPN vs Port Forwarding

VPN vs Port Forwarding: Which Method is best for delivering Remote Access to home or Small Office Networks

Martin Boulter, Luxul Customer Services Manager

Installers of home and small office networks are often asked by customers for the ability to access their private local-area network (LAN) remotely via the Internet. Such remote connections are convenient and often necessary for frequent travelers, as well as for geographically dispersed locations or employees. Installers and service providers might also use a remote network connection to provide better customer service, troubleshoot network problems and resolve issues without the need to send a technician onsite.

There are several methods for implementing a remote network connection. The two most common methods are Port Forwarding and Virtual Private Networking (VPN). In this article, these two methods will be discussed and compared. Which method an installer elects to use may depend upon the features supported by the equipment being installed. A professional grade router such as Luxul's XBR-2300 (which supports both methods) is typically required.

Port Forwarding and VPN Definitions

Port Forwarding: Allows remote computers to pass data to a specific computer or service within a private local-area network (LAN) by mapping traffic crossing specific ports to specified devices on the network. With Port Forwarding, the router is set to listen on a specific port for inbound traffic. If that port is contacted, information is then forwarded to the mapped internal resource.

VPN (Virtual Private Network): A VPN allows the user to access the private local-area network (LAN) as if physically connected at the site. Unlike Port Forwarding, a VPN provides multiple levels of security through tunneling protocols and security procedures such as password verification and encryption.

Image 1: Luxul XBR-2300 Enterprise Dual-WAN Router

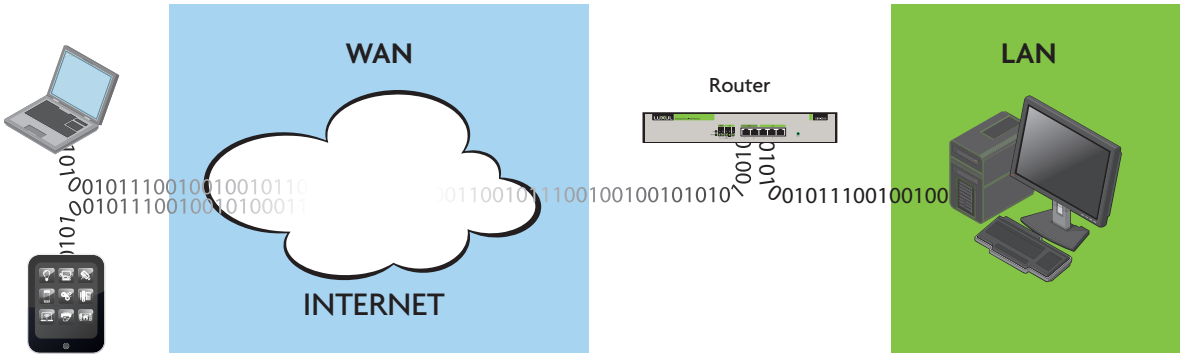

Image 2: Port Forwarding

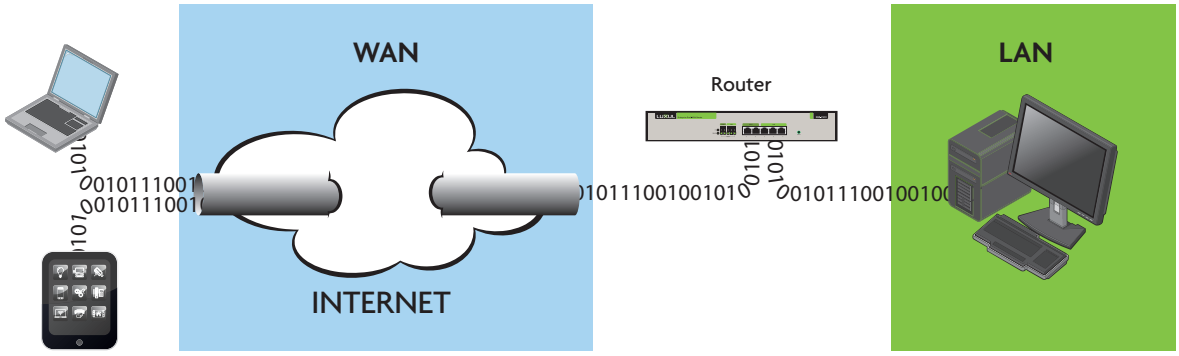

Image 3: VPN

Port Forwarding Pros

- Easy to configure. Only requires device IP Address and the Port it is listening on.
- Ability to create multiple rules. Most routers will allow the creation of multiple port forwarding rules—even to the same device.
- Forwards the user to the private network without requiring a password
- Works with Dynamic DNS

Port Forwarding Cons

- Not secured in any way. Unless data from the internal network resource is encrypted, all data being passed is open for anyone to see.
- Hackers can easily scan for open ports that can be used for breaking into internal systems
- Rules must be created for each device and internal resource
- Changing or adding rules may require additional site visits.

VPN Pros

- Moderately simple configuration. User information is required, but no need for internal resource information.
- 1st Level of Security: There is only one open port which is username and password protected.
- 2nd Level of Security: All traffic to and from private network is encrypted.
- 3rd Level of Security: Internal resources are password protected.
- Allows access to all ports and internal resources—not just the few devices for which rules are created.
- Works with Dynamic DNS
- Most OS's and devices natively support the most popular VPN types without additional client software.

VPN Cons

- Connecting to internal resources is now a two step process. The user must login to the VPN connection and then to the internal resource.
- Uses secure username and password, which can be forgotten.
- Traffic to and from the internal network may be slightly slower due to the encryption process.
- Some VPN setups may require separate client software to connect.

While there are positive and negative aspects of both methods, there are some major differences when it comes to security. Port Forwarding passes all data in what is referred to as "the clear," which means packets can be captured and analyzed without much effort—providing a rather open door into the system for a skilled hacker. On the other hand, while a VPN requires additional steps to connect to the network, it provides superior security. Plus, with a VPN, all of the data is encrypted—making the information much more difficult to use if somehow it is intercepted.

Although Port Forwarding makes sense in certain applications and installations, to minimize security risks, Luxul normally recommends using a VPN. We also do our best to make VPN setup as simple and hassle free as possible. A typical VPN setup using a Luxul XBR-2300 router requires only three steps:

- Initialize the VPN Server: This step includes setting the VPN Server IP address, creating a DHCP pool to be used by connecting clients, and choosing the desired encryption type.
- Create User Accounts: Input a user name, create a password for the user, and select if the user will have access to the local network or just to the router.
- Configure the Client Device: Most Operating Systems now natively support a VPN client that is capable of connecting to the most popular VPN types. For client devices with native VPN support, all that is required is Server Address, User Name, and Password.

More information about setting up a VPN can be found at: *luxul.com/how-to-videos*

The need for secure remote access to private LAN resources is no longer limited to large corporations with satellite locations or mobile employees. A growing number of homeowners and small business owners now have the same requirement. At the same time, many service providers use remote access to their customer's network as a way to improve customer service while minimizing costs. By understanding how to configure and use a VPN, savvy network installers have one more tool for adding value to their customers.

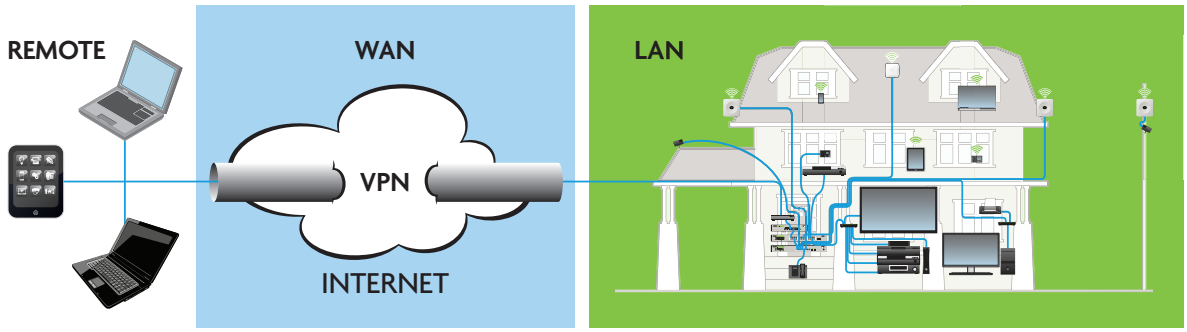

Image 4: Typical VPN Topology