A VPN can be implemented as software on the host and gateway or as a hardware appliance. The problem remote users face is that their communications are open on the long stretch of the public or unsecure network from the laptop or home computer to the work environment. One solution to minimize the risk of hacking is to install a leased line, which has the advantage that only a physical attack on it can compromise security; however, this is the most expensive of all VPN options. The major disadvantage of leased lines is that you can have only a limited number of physical leased lines and the installation of leased lines is extremely time-consuming and expensive.

**VPN Appliance**

The general structure of VPN communication is as follows:

![VPN Diagram](image)

A remote user, such as a home user, connects to the network via the Internet, a firewall, and a VPN. These VPN appliances come in all shapes and sizes. Some firewalls have a VPN built into them, while some stand-alone VPN appliances work in conjunction with a firewall. The larger the number of remote users, the more likely the network will require a dedicated VPN.

**VPN Hosts and Trust**

Trust-based access varies depending on who is allowed through the VPN. The various levels of VPN hosts and trusts are as follows:
With each level, the IT department has less control. The first level might be an employee on a hotel network. At home, the employee should be following an IT policy. However, the employee also has, potentially, a family or a roommate and friends and neighbors who might have access. In addition, there is the risk of physical breach. A policy may be sufficient in mitigating these risks if the employee is trustworthy.

Airport networks are improving every day, and many are at the level of a managed network. The disadvantage is that the employee is out in the open and subject to surveillance. Authorized partners and customers are more of a risk because there is no expectation of corporate policy controls. We have to assume they will act autonomously and may represent an increased risk.

**VPN or Firewall Security**

Some of the security strategies for VPN and firewall implementation are as follows:

- Do not implement a VPN with no firewall; for a VPN, a firewall is the best protection and they both complement each other.
- Keep the VPN behind the firewall or use a firewall or VPN appliance.
- Make sure your operating system is Internet Protocol Security (IPSec) compliant.

Keep in mind that VPNs produce a security overhead that may affect network Internet bandwidth. In the case of a wireless local area network (LAN), ensure that you:

- Place a wireless access point outside the firewall.