



## Basic VPN setup.

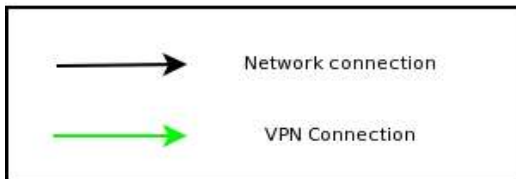
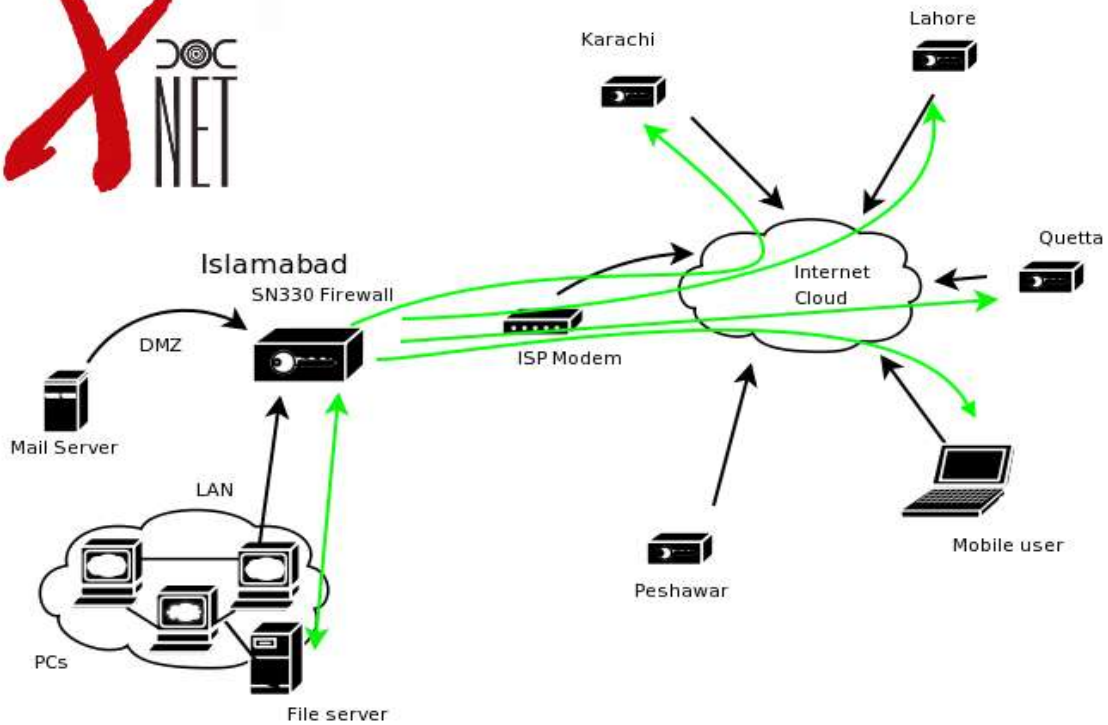
VPNs come into the picture when the corporate network is divided into geographically diverse subnets and you need to connect these to allow data sharing. VPN functionality is in addition to the access control functions. Both functions are provided simultaneously without mutual interference. In fact an existing resource (access to the Internet) is utilised in a more productive manner.

A VPN connection allows data transfer (for example, file sharing) over the Internet while transparently encrypting the data transmission. The point being that the remote computer looks like it is attached to the local LAN.

There are 2 kinds of VPN connections:

- 1 Permanent connections between Firewalls. These are called Tunnels and are used to connect 2 offices together. A number of tunnels may be set-up on each Firewall. Each Firewall should be connected to the Internet via a high speed connection, such as DSL.
- 2 Temporary connections between a Firewall and a mobile user. The mobile user may be working from a PC at home or from a Laptop while travelling. The mobile user will usually connect using a normal dial-up account over PSTN, though any Internet connection may be used.

Some ISPs provide what they describe as VPNs but these are generally just leased lines where the data is transmitted in cleartext form and not encrypted. This is obviously not secure. Other ISPs will setup a VPN for you, but again if the encryption is handled by a third party then you should understand the security implications of such an arrangement.



Virtual Private Network representation  
<http://www.Xnet.com.pk/>

The above diagram illustrates that remote users are able to access the Fileserver and Mailserver in Islamabad in a secure manner. The remote LANs (for example in Lahore) can access these servers as if they are in the Local LAN in a transparent manner.

The Xnet Solutions SN330 hardware firewall is able to provide 3Mbps of throughput using AES (AES has replaced DES and 3DES as the algorithm approved by the US Government for its own use with classified data).

VPNs are also used to secure remote office wireless connectivity. Wireless connectivity is usually very insecure and it is recommended that it be encrypted.