





Legend

Inter-connection

A **virtual private network (VPN)** connection is a secure "tunnel" formed between a private network and a remote machine connected anywhere on the Internet. The server controlling the connection and the remote machine can reside on the same network, or they can be. The most important thing to remember is that a VPN connection requires an active Internet connection. The networks will need to connect to your ISP normally before establishing a VPN connection.

As we know, data traffic consumes **bandwidth**, a measure of how much information can be sent over a network during a specific unit of time. Bandwidth is usually measured in megabytes per second, or Mbps. If too much data flows through a network, the network can experience **lag** or delays in response times. To alleviate lag and conserve bandwidth, the network VPN will support the concept of **split tunneling** for connected users. Simply defined, this means that some of the data will travel through the VPN tunnel, while the rest will travel over the normal, unencrypted connection. What this means is that whenever a user activates the VPN connection from a remote location, the data's destination is categorized before any data is sent over the Internet. The VPN client software checks all outbound traffic to see whether or not that data is headed for campus. Based on that check, the VPN client addresses your packet in one of two ways:

- **eHealth Management traffic** - All data that is destined for the Health Management Network will be addressed so that it is delivered to the VPN server located at either EAC Secretariat or the various Ministry of Health offices. The data packets are encrypted before being forwarded to the regular network adapter of the computers that belong to the network. Each encrypted packet includes the final destination address for that packet.
- **Non-EAC network traffic** - Any data that is not related to the Health Management Network and service is not addressed for delivery to the network. Therefore, it will travel normally from machines belonging to the network to the ISP and then makes its way to its eventual destination. This keeps your non- Health Management Network activities private and conserves bandwidth on the Health Management Network.

Network Composition

The Wide Area Network will comprise of different country networks that will in turn comprise of hospital networks interconnected to the main country node located in the various Ministry of Healths through VPN Tunnels which are secure. The Ministry of Health central nodes will be

linked to the EAC Health secretariat which will in turn be linked to the WHO head office through the normal internet channels but using secure VPN Tunnels.

The hospital network will comprise two computers with one computer acting as a server. The Ministry of Health office network will have two computers each and a small server. This will enable the data that will be collected from the hospitals to be forwarded to EAC Health Secretariat. The EAC secretariat will have more computers plus a powerful server that will be receiving data from the ministry of health for each country, process the data and then forward them to the MOH and then to the hospitals.