VIRTUAL PRIVATE NETWORKS - I

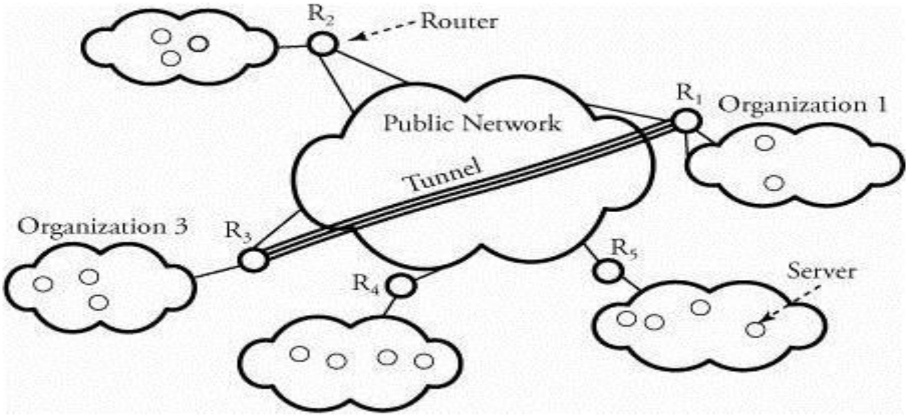
A virtual private network (VPN) is a data network having connections that make use of public networking facilities. The (VPN) part of public network is set up "virtually" by a private-sector entity to provide public networking services to small entities. With the globalization of businesses, many companies have facilities across the world and use VPNs to maintain fast, secure, and reliable communications across their branches.

VPNs are deployed with privacy through the use of a tunneling protocol and security procedures. It shows two organizations, 1 and 3, connected through their corresponding routers, forming a tunnel in the public network, such as the Internet. Such a structure gives both private organizations the same capabilities they have on their own networks but at much lower cost. They can do this by using the shared public infrastructure. Creating a VPN benefits an organization benefits by providing

- Extended geographical communication
- Reduced operational cost
- Enhanced organizational management
- Enhanced network management with simplified local area networks
- Improved productivity and globalization

But since each user has no control over wires and routers, one of the issues with the Internet is still its lack of security, especially when a tunnel is exposed to the public. Thus, VPNs remain susceptible to security issues when they try to

Figure 6.6. Two organizations connected through a tunnel using public facilities



connect between two private networks using a public resource. The challenge in making a practical VPN, therefore, is finding the best security for it. Before discussing VPN security, we focus on types of VPNs. There are two types of VPNs each determined by its method of tunneling, remote-access and site-to-site. We will explain these two approaches in the next two sections.

Remote-Access VPN

Remote-access VPN is a user-to-LAN connection that an organization uses to connect its users to a private network from various remote locations. Large remote-access VPNs are normally outsourced to an Internet service provider to set up a network-access server. Other users, working off campus, can then reach the network-access server and use the VPN software to access the corporate network. Remote-access VPNs allow encrypted connections between an organization's private network and remote users through a third-party service provider. Tunneling in a remote-access VPN uses mainly the Point-to-Point Protocol (PPP). PPP is the carrier for other Internet protocols when communicating over the network between a host computer and a remote point. Besides IPsec, other types of protocols associated with PPP are L2F, PPTP, and L2TP. The Layer 2 Forwarding (L2F) protocol uses the authentication scheme supported by PPP. The Point-to-Point Tunneling Protocol (PPTP) supports 40-bit and 128-bit encryption and uses the authentication scheme supported by PPP. The Layer 2 Tunneling Protocol (L2TP) combines features of both PPTP and L2F.

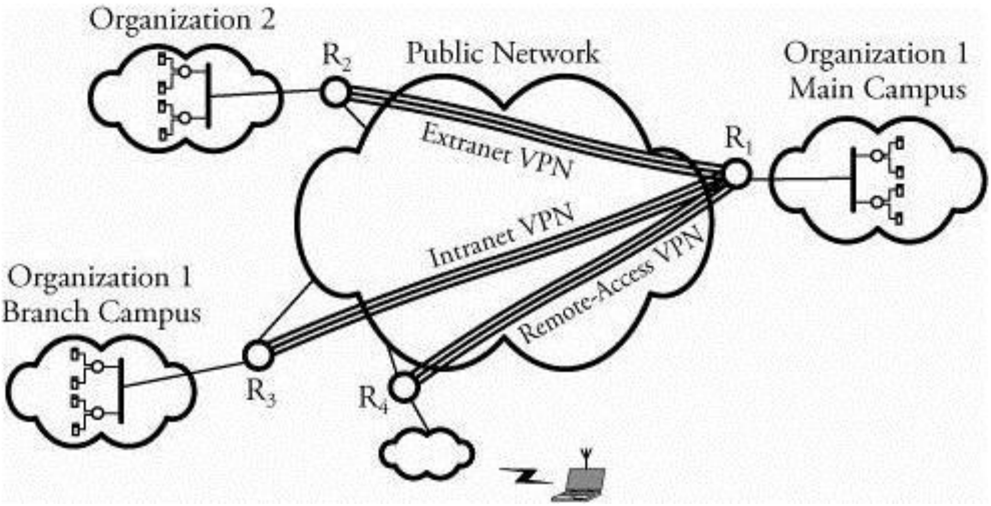
Site-to-Site VPN

By using effective security techniques, an organization can connect multiple fixed sites over a public network. Site-to-site VPNs can be classified as either intranets or extranets.

- Intranet VPNs connect an organization's remote-site LANs into a single private network.
- Extranet VPNs allow two organizations to work in a shared environment through a tunnel built to connect their LANs.

Figure 6.4 shows the three types VPNs discussed so far. Organization 1's main campus and branch campus are connected through an intranet VPN tunnel. The main campus can also be connected to organization 2 through an extranet VPN tunnel. The employees of organization 1 can also access their corporation through a remote-access VPN. Each remote-access member must communicate in a secure medium. The main benefit of using a VPN is scalability with a reasonable cost. However, the physical and virtual distances of two communicating organizations have a great impact on the overall cost of building a VPN.

Figure 6.4. Three types of VPNs to and from a headquarter organization



In a site-to-site VPN, generic routing encapsulation (GRE) is normally the encapsulating protocol. GRE provides the framework for the encapsulation over an IP-based protocol. IPsec in tunnel mode is sometimes used as the encapsulating protocol. IPsec works well on both remote-access and site-to-site VPNs but must be supported at both tunnel interfaces. The Layer 2 Tunneling Protocol (L2TP) can be used in site-to-site VPNs. L2TP fully supports IPsec regulations and can be used as a tunneling protocol for remote-access VPNs.

Source : http://elearningatria.files.wordpress.com/2013/10/cse-vi-computer-networks-ii-10cs64-notes.pdf