Davison Bullock MSc IT PT

21/01/2013 1500 words

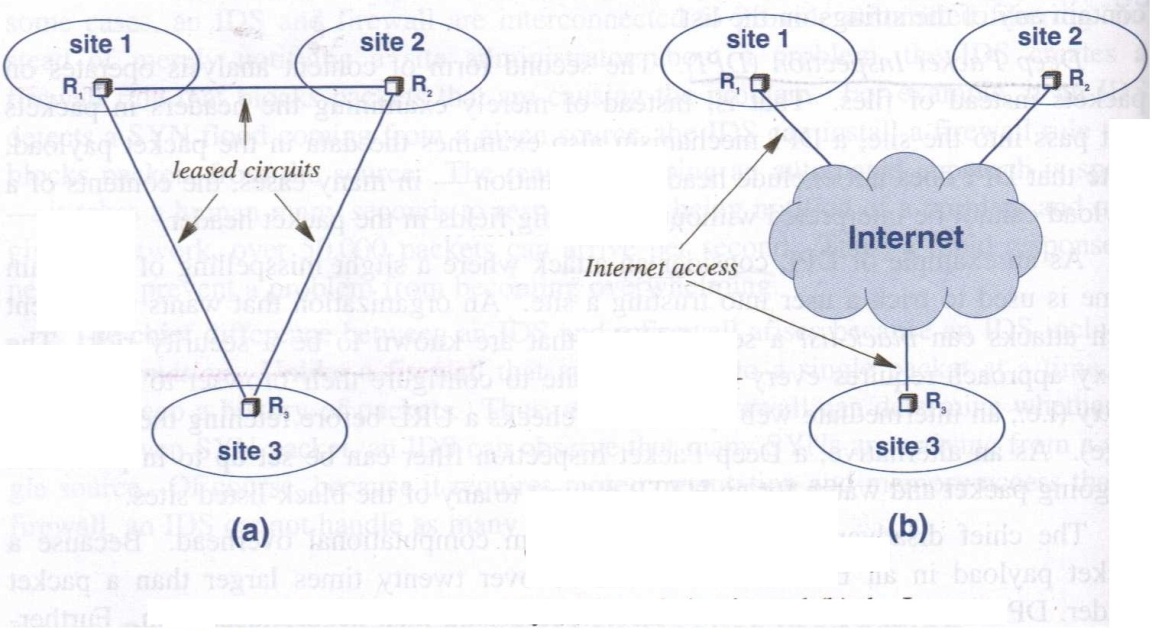
I confirm that this report is entirely my own work, except where explicitly stated otherwise.

**Virtual Private Networks (VPN)**

**1. The purpose of VPN.**

Virtual Private Network (VPN) allows computers and networks to be connected to each other over the transport layer by using un-trusted media like the internet (Ref 13). It extends a private network and its resources (including routers, links and DNS infrastructure) (Ref 9) across public networks as a wide area network (WAN) but appears like a private network link to the user with its security, functionality and management policies (Ref 4 and Ref 15).

Traditionally sites connected via leased data circuits by connected routers (R) at each of the sites and passing data across these circuits (Fig 1 (a)). VPN combines data transfer between sites using the low cost public internet (Fig 1 (b)) without using expensive leased lines and making sure data is kept private during transmission (Ref 4).



**Figure 1 - Sites connected by (a) leased circuits and (b) the Internet (Ref 4)**

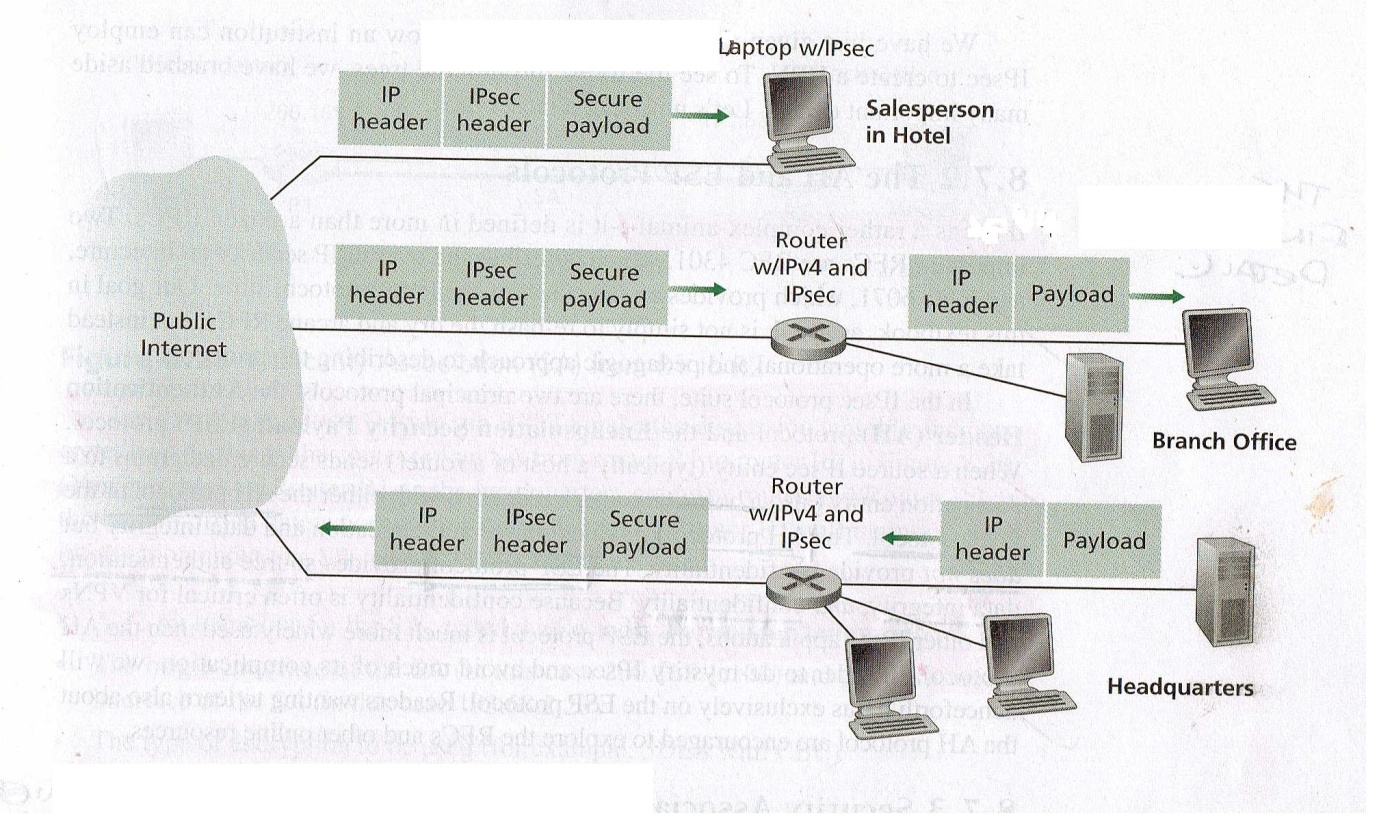
VPN is often used by telecommuters using a **standalone device** (VPN router) that creates a secure communication to the organisations VPN Server. Alternately **VPN software** can be used (Ref 4).

**2. VPN protocols compared (Ref 1, Ref 11, Ref 8, Ref 14, Ref 12, Ref 17, Ref 18 and Ref 19):**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **PPTP** | **L2TP/IPSec** | **SSL/OpenVPN** |
| **Description** | Point to Point protocol uses control channel over TCP and a GRE tunnel to encapsulate PPP packets. No standard. | Layer 2 Tunnelling Protocol for Point to Point communication.  LT2P No Encryption  Uses control and data packets | Open source application and implements VPN. |
| **Operates on OSI Model** | Layer 2 | Layer 2 | Layer 2 and 3 |
| **Encryption** | 128 bit  No encryption relies on tunnelling. GRE Tunnel tunnels any protocol  Fast reliable speeds | Uses 256 bit  IPSec | Uses 256 bit  Open SSL encrypted data and control channels.  Fast / reliable over great distances and high latency networks. |
| **Authentication** | None. Relies on tunnelling. MS Windows allows PPTP security. | Pre-shared keys.  IPSec. | Pre shared keys, certificates  Depends on third party modules |
| **Networking** | PPTP tunnel created by communicating with port 173.  GRE tunnel is created next and uses PPTP GRE packets. PPTP tunnel allows any protocol to be carried in PPP packet. | Bi directional network traffic in tunnel. PPP in tunnel allows networking. LT2P is sent through IP tunnel using UDP. | Runs over UDP or TCP transport through multiplexing SSL tunnels.  Suitable alternative to LT2P/IPSec  Offer 2 network interface types |
| **Security** | Not Secure | Good security and reliability for control packets. Tunnelling provides reliable packets | Runs in user space. IP Stack not needed. Protocol based on SSL and TLS.  Supports smart card |
| **Extensibility** | N/A | Tunnelling of nested protocols | Enhanced security through plug-ins and scripts |
| **Advantage** | Uses TCP allowing lost data retransmission (Ref 14) | Harder to intercept and crack data during transmission (Ref 14) | Available in most web browsers. Cheaper to set up (Ref 14 and Ref 10).  Offers precise access control to applications rather than whole network like IPSec  Allows longer stronger key (Ref 12) |
| **Disadvantage** | Least encrypted form of VPN  Only user level authentication (Ref 14). | Problem if key infrastructure is down.  Same key needed on connection ends (Ref 3) | Need powerful computers for VPN for latency or delay in network (Ref 14).  Can only access applications through web browser.  Network resource un-shareable (Ref 3) |
| **When to use** | When OpenVPN is not available. Where speed and ease of use is required (Ref 6). | Better security than PPTP (Ref 3). | Access to applications through a web browser and when a low cost VPN is required (Ref 3) |

**3. Implementation of L2TP/IPSec VPN.**

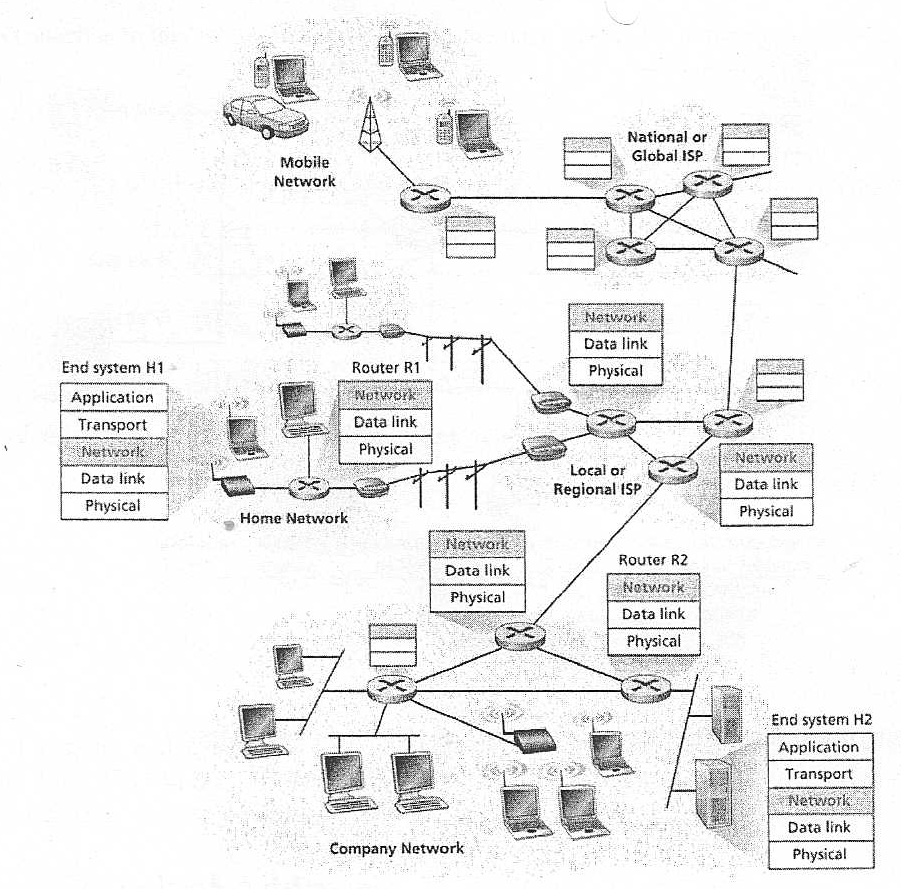
When two hosts send data to each other in the headquarters site an IPv4 datagram is used. The gateway router in the organisations site encrypts IPv4 datagram to IPSec datagram before sending over the public internet i.e. in the case of the remote user (Ref 9).



**Figure 2. VPN (using IPSec protocol) (Ref 9)**

The IPSec datagram contains an IPv4 header to allow IPv4 routers in the internet to process the datagram. The IPSec datagram's payload (data) is encrypted using IPSec and includes an IPSec header allowing IPSec compatible network parts to process it (Ref 9).

The IPSec datagram is sent from the organisation to a remote user via the internet (via Layer 3 - network layer using internet protocols) and is decrypted by the remote host operating system (end point) and IPSec services allows data integrity verification and unencrypted payload data to pass to the TCP of UDP transport layer protocols above it .



**Figure 3 - TCP/IP model layers for networked devices (Ref 9 )**

**A LT2P/IPSec VPN is implemented by:**

1.Negotiation of IPSec security associations

Before IPSec datagram's are sent between pairs of network entities via TCP on the transport layer (Step 3) a network logical connection is created between entities called a **Security Association (SA)** (through Internet Key Exchange(IKE)) allowing each entity to send to a secure datagram in each direction (Ref 9) done over UDP port 500 (Ref 18) with shared and public keys and certificates at both ends. Two logical connections (SA's) are required. An organisations gateway router maintains state information about the SA (Ref 9)

2. The ESP communication in transport mode is established next which offers authentication. The IP protocol number is 50 for ESP. This creates a secure channel but tunnelling does not take place yet (Ref 18).

3. Next the L2TP tunnel between SA end points is established by negotiation of parameter over the SA secure channel and within the IPSec encryption. LT2P uses UDP port 1701 (Ref 18).

A sending router uses state information to construct an IPSec datagram to forward over SA. The receiving router uses this to authenticate and decrypt arriving IPSec datagram's from the SA.

IPSec entities (Hosts and Routers) maintain state information for many SA's (Ref 9).

IPSec has **Tunnel Mode** and **Transport Mode** packet forms.

An IP header is created with IPv4 header fields appended. The IPSec datagram header fields from IPv4 is followed by a payload (ESP header, IP datagram, ESP trailer, ESP authentication field) (Ref 9).

Original IP datagram addresses are encrypted and stored in IPSec packet payload. The new header of the IPSec packet contains addresses for the router interfaces at either end of the tunnel. NB. IPv4 header fields protocol number 50 is used for ESP (Ref 9, Ref 18).

4.After the source router sends the datagram into the internet it passes multiple routers processing as a normal datagram (unaware IPSec encrypted data is carried). The destination IP address is the outer header for these public internet router which gets packet to its destination (Ref 9).

**4. Problems and drawbacks of using VPN technologies**.

* VPN performance problems from lower internet throughput (some applications work better on a LAN than when connected to remotely), longer delay (due to number of traversals) and high overhead compared to a direct connection (Ref 4).
* Knowledge of networking and security is required to install and configure VPN over a public network otherwise can lead to poor security protection (Ref 2, Ref 9).
* The VPN is based on the performance and reliability of the internet which is controlled by the ISP. Users may have trouble staying connected to the VPN (Ref 2, Ref 9, Ref 5). Companies can agree an SLA with the ISP to guarantee performance (Ref 5).
* VPN technologies from vendors can be incompatible due to issues with VPN standards (Ref 2).
* Remote workers home computers may have security weaknesses (Ref 2). Having a firewall installed reduces security threat (Ref 4).
* Roaming across access points with wireless devices can break VPN solution because of higher level encryption used in VPN (Ref 5). Adding routers improves reliability (Ref slides).

**5. Known security issues with VPN.**

**Security Threat to VPN elements**

**VPN client software** uses a username and password. Password protection, access control list that controls applications user access and use of password protected screensavers can all reduce security threat (Ref 7).

A VPN might have **ISP Segment** and **Malicious routers and malicious ISP** that allow data interception and examination of encrypted packet data or malicious data to enter network. Strong encryption protocol's in VPN elements can prevent threats (Ref 7).

**VPN protocol(s) attacks**

Protocols are vulnerable to data packet and password interception i.e. PPTP sends passwords in the clear (Ref 7).

**Cryptanalysis attacks**

Attackers can break key codes/ciphers to decipher message from data passed from sender to receiver without knowing cryptographic keys used. Strong key encryption can reduce this threat (Ref 7).

**Denial of Service attacks.**

Attackers use viruses, malware and impersonation to access or damage resources causing network congestion and targeted computers to crash. IP packets size are tampered with due to lapses in the communication technologies. D.o.S. attacks countered by backups, password policies, route filters to filter fragmented packets, disable unused network services, controlling resources, filters for IP spoofed packets, patches, firewall and Intrusion Detection System (Ref 4, Ref 7).

**References**

1. Allen, M. (2001). *Virtual Private Networking - The CTDP Networking Guide Version 0.6.3.* Available: http://www.comptechdoc.org/independent/networking/guide/netvpn.html. Last accessed 24th December 2012.

2. Bradley, M. (2012). *What Are the Advantages and Benefits of a VPN?.*Available: http://compnetworking.about.com/od/vpn/f/vpn\_benefits.htm . Last accessed 6th Jan 2013.

3. Bradley, T. (2012). *VPN's: IPSec vs. SSL Which Technology Is Right For You?.* Available: http://netsecurity.about.com/cs/generalsecurity/a/aa111703.htm. Last accessed 13th Jan 2013.

4. Comer, D (2009). *Computer Networks and Internets*. 5th ed. River Saddle, NJ. USA: Pearson Education. 525-532.

5. Edwards, J. (2011). *VPN: The Pros and Cons.* Available: http://www.itsecurity.com/features/vpn-popularity-021108/. Last accessed 7th Jan 2012.

6. Golden Frog. (2012). *VPN Protocol Comparison - PPTP vs. L2TP vs. OpenVPN.* Available: http://www.goldenfrog.com/vyprvpn/pptp-vs-l2tp-vs-openvpn . Last accessed 6th Jan 2013.

7. Gupta, M (2002). *Building a Virtual Private Network*. India: Prima Tech. Part IV.

8. Hsieh , J. (2012). *Difference between OpenVPN, PPTP, L2TP, IPSec.*Available: http://blog.ijun.org/2012/02/difference-between-openvpn-pptp-ipsec.html. Last accessed 6th Jan 2013.

9. Kurose, J and Ross, K (2012). *Computer Networking: A Top-down Approach*. 6th ed. Harlow: Pearson. p744-750.

10. Mitchell, B. (2012). *What Are the Key VPN Security Technologies?.*Available: http://compnetworking.about.com/od/vpn/f/vpn-security.htm. Last accessed 13th Jan 2013.

11. Netgear. (2012). *What is VPN (Virtual Private Networking)?.* Available: http://kb.netgear.com/app/answers/detail/a\_id/1128/~/what-is-vpn-(virtual-private-networking)%3F. Last accessed 24th December 2012.

12. ST4RTvpn. (2012). *What are the three main VPN protocols?.* Available: http://www.start-vpn.com/blog/VPN-protocols/. Last accessed 6th Jan 2013.

13. telecomsoftware. (2009). *VPN and its purpose.* Available: http://www.telecomsoftware.biz/VPN-and-its-purpose.html . Last accessed 24th December 2012.

14. TheVPNAdmin. (2012). *Advantages and Disadvantages of PPTP, L2TP, SSTP, and OpenVPN.* Available: http://www.squidoo.com/advantages-and-disadvantages-of-vpn-protocols. Last accessed 6th Jan 2013.

15. Various. (2012). *Virtual private network.* Available: http://en.wikipedia.org/wiki/Virtual\_private\_network. Last accessed 6th Jan 2013.

16 Wisegeek. (2012). *What Are the Disadvantages of a VPN?.* Available: http://www.wisegeek.com/what-are-the-disadvantages-of-a-vpn.htm. Last accessed 6th Jan 2013.

17. Various. (2012). *Point-to-Point Tunnelling Protocol.* Available: http://en.wikipedia.org/wiki/Point-to-Point\_Tunneling\_Protocol. Last accessed 20th Jan 2013.

18. Various. (2012). *Layer 2 Tunnelling Protocol.* Available: http://en.wikipedia.org/wiki/Layer\_2\_Tunneling\_Protocol. Last accessed 20th Jan 2013.

19. Various. (2012). *OpenVPN.* Available: http://en.wikipedia.org/wiki/OpenVPN. Last accessed 20th Jan 2013.