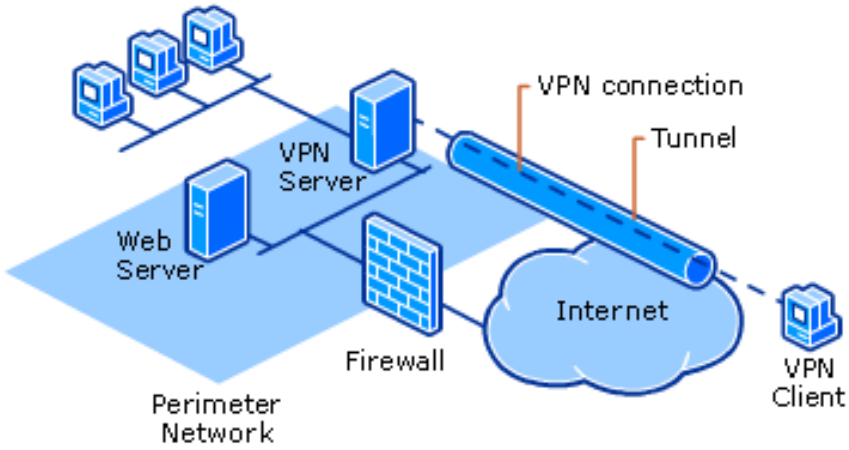
VPN

Virtual Private Network

What is VPN

- Extension of a private network that encompasses links across shared or public networks like the Internet.
- Enable to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.

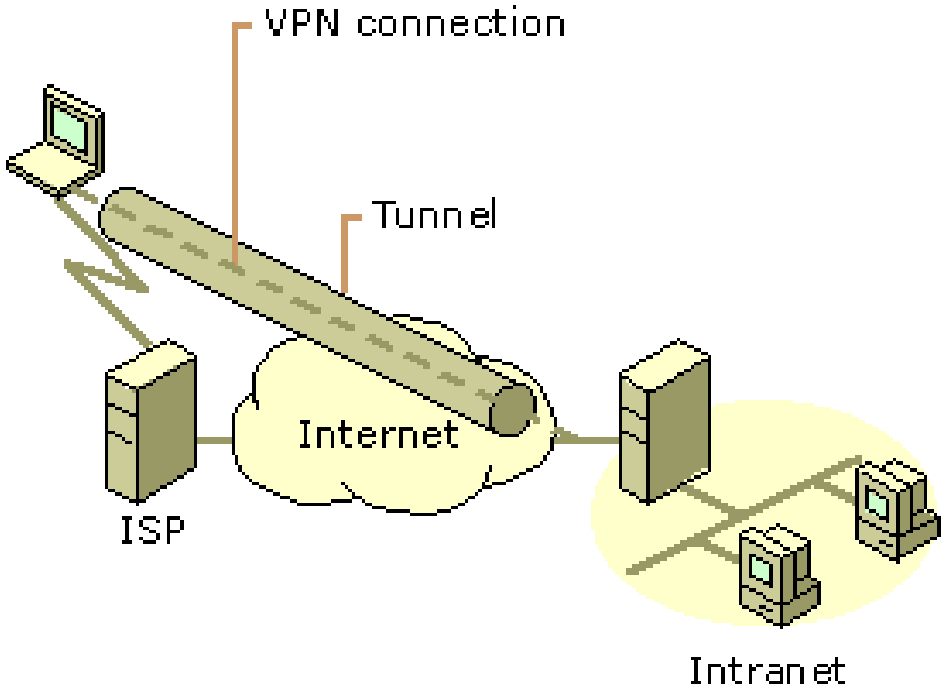


Why ?

- Cheap
  - Legacy private network uses remote connectivity through dial-up modems or through leased line connections, it's expensive.
- Scalable
  - Extending a leased line connection is complex.
  - Easy to administer.
- Security
  - Provide encryption and file integrity.

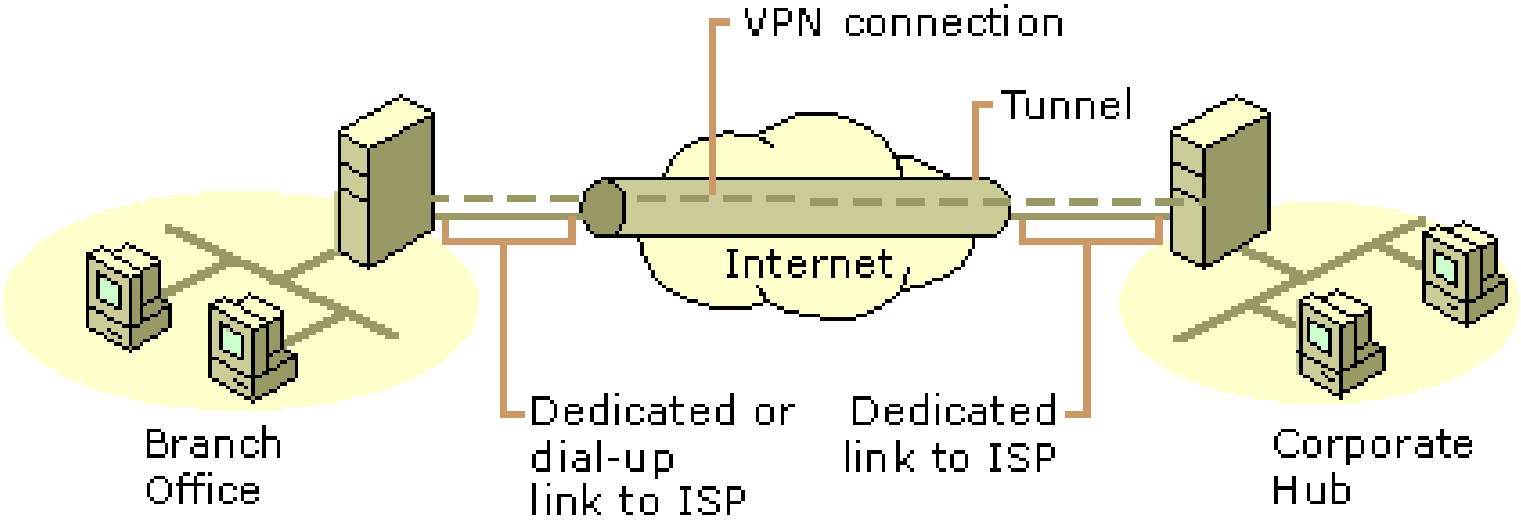
Common Uses of VPNs – 1

- Remote Access Over the Internet



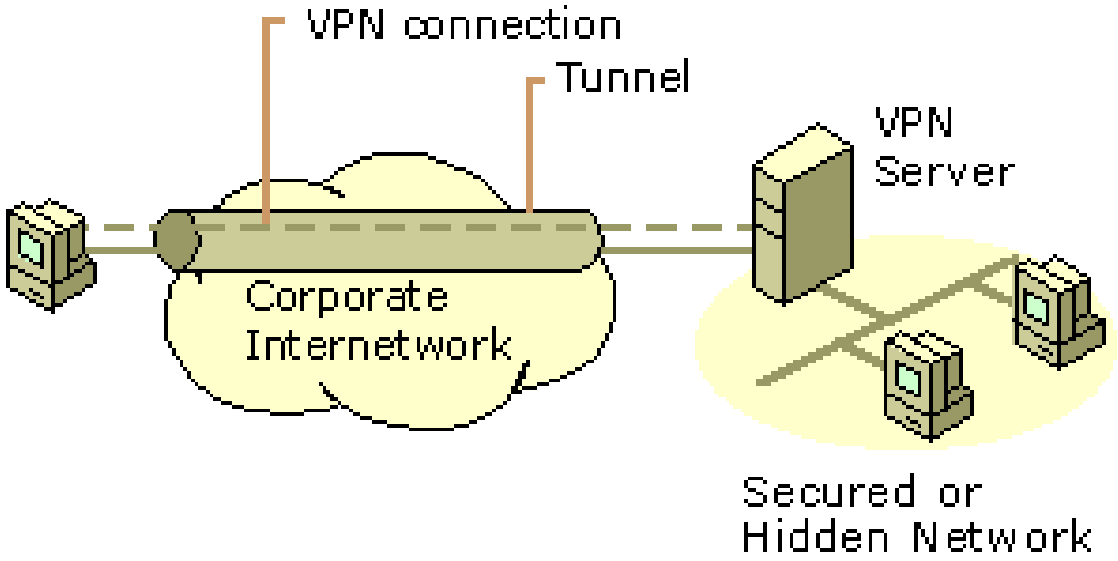
Common Uses of VPNs – 2

- Connecting Networks Over the Internet (Site to Site VPN)



Common Uses of VPNs – 3

- Connecting Computers over an Intranet



Basic VPN Requirements

- User Authentication
- Key Management
- Address Management
- Data Encryption

Basic VPN Requirements – 1

- User Authentication
  - Verify the VPN client's identity and restrict VPN access to authorized users only.
  - Provide audit and accounting records to show who accessed what information and when.
  - X.509, pre-share key….
- Key Management
  - Generate and refresh encryption keys for the client and the server.
  - Simple Key Management for IP, ISAKMP/Oakley…

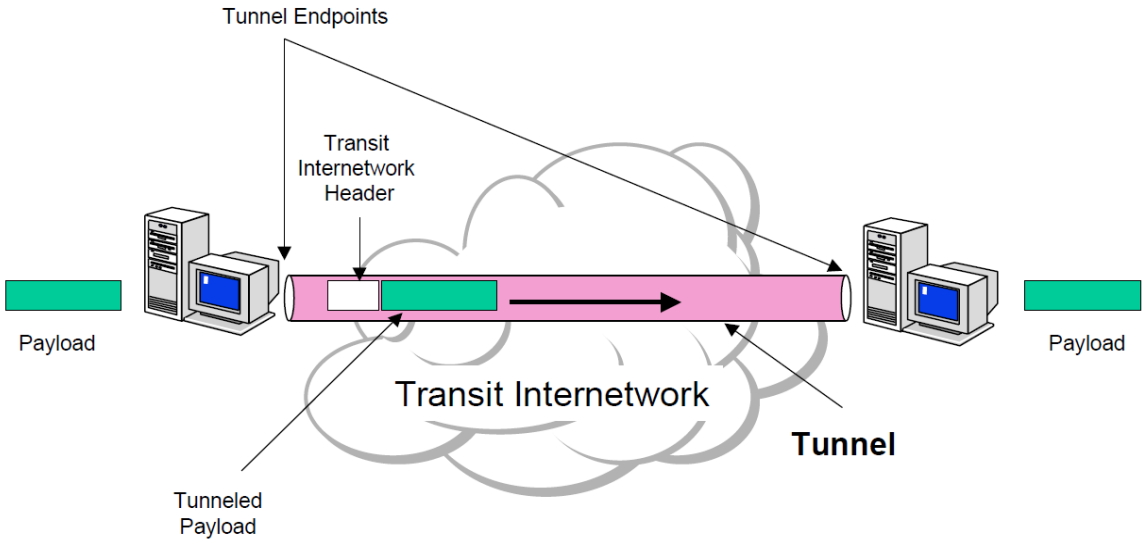
Basic VPN Requirements – 2

- Address Management
  - Assign a VPN client's address on the intranet and ensure that private addresses are kept private.

- Data Encryption
  - No one outside the VPN can alter the VPN.
  - Data carried on the public network must be rendered unreadable to unauthorized clients on the network.

Tunneling

- VPN consists of a set of point to point connections tunneled over the Internet.
- In order to achieve tunneling, the packets are encapsulated as the payload of packets.
  - Payloads, to and from addresses, port numbers and other standard protocol packet headers
  - As seen by the external routers carrying the connection



Common Implementations

- Point-to-Point Tunneling Protocol (PPTP) [RFC 2637]
- Layer Two Tunneling Protocol (L2TP) [RFC 2661]
- IPSec Tunnel Mode [RFC 2401]
- Secure Socket Tunneling Protocol (SSTP) [Spec]
- BGP/MPLS IP VPN [RFC 4364]
- SSL VPN

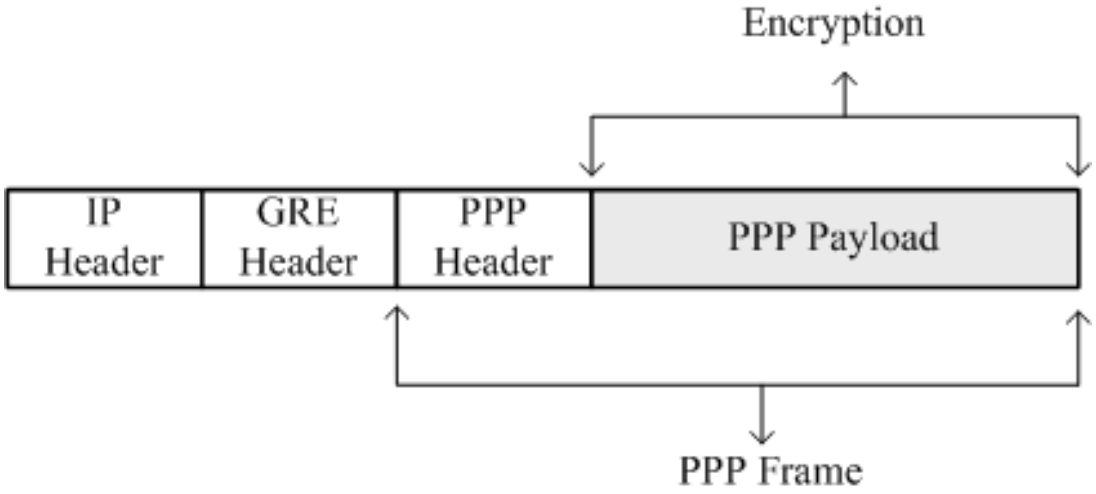
…, etc

PPP

- Point-to-Point Protocol [RFC 1661]
- PPP was designed to send data across dial-up or dedicated point-to-point connections.
  - PPP encapsulates IP, IPX, and NetBEUI packets within PPP frames, and then transmits the PPP-encapsulated packets across a point-to-point link.
- User Authentication
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
  - M$ Challenge Handshake Authentication Protocol (M$-CHAP)
  - M$-CHAPv2
- Data can be compressed or encrypted before transmission.
  - Microsoft Point to Point Compression / Encryption (MPPC / E)

PPTP

- Point-to-Point Tunneling Protocol
  - PPTP doesn't describe encryption or authentication
    - Rely on the PPP protocol
  - PPTP encapsulates PPP frames in IP datagrams for transmission over an IP internetwork by TCP connection.
  - PPTP uses a modified version of Generic Routing Encapsulation (GRE) to encapsulate PPP frames for tunneled data.

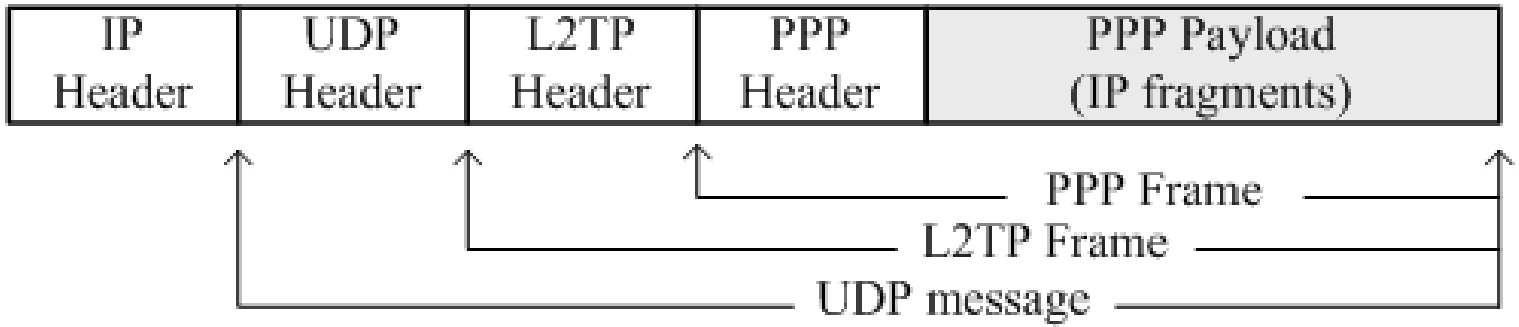


Security of PPTP

- PPTP has been the subject of many security analyses and serious security vulnerabilities have been found
  - MS-CHAP is fundamentally insecure.
  - MS-CHAPv2 is vulnerable to dictionary attack on the captured challenge response packets.
- EAP-TLS (Extensible Authentication Protocol – TLS) is the superior authentication choice for PPTP.

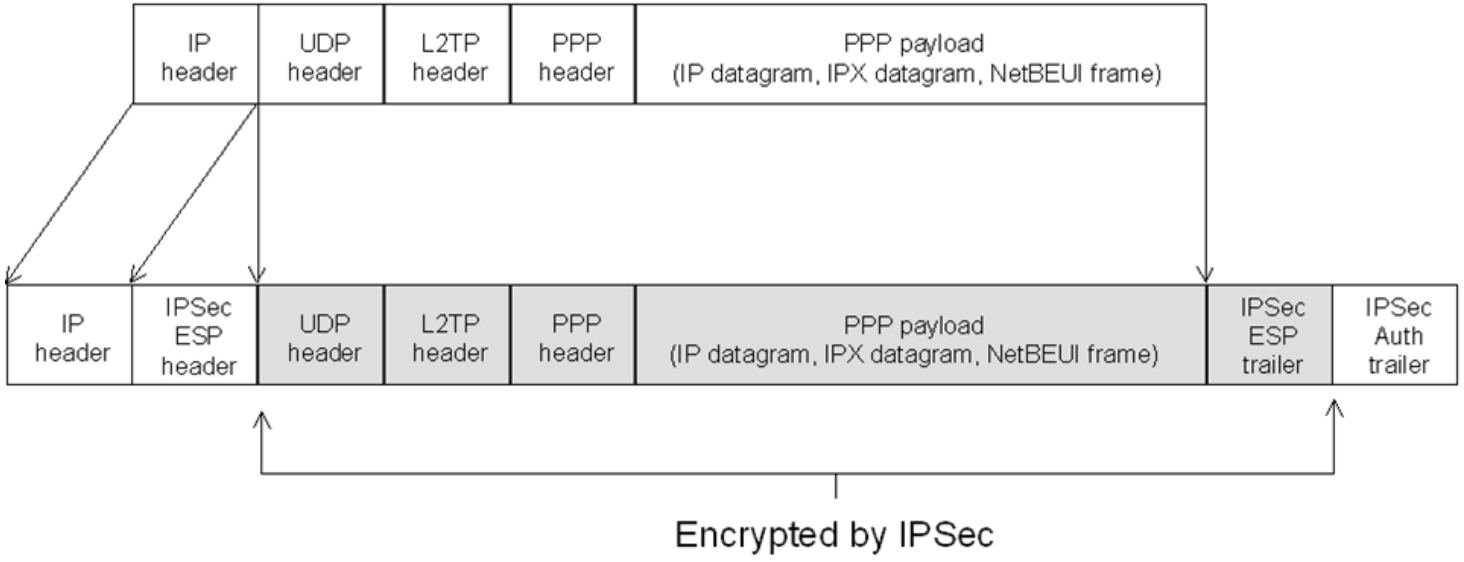
L2TP

- Layer Two Tunneling Protocol
  - PPTP+L2F (Layer Two Forwarding)
  - L2TP over IP internetworks uses UDP and a series of L2TP messages for tunnel maintenance.
  - A tunnel can contain multiple connection at once.



L2TP/IPsec

- Usually use IPsec ESP (Encapsulating Security Payload) to encrypt the L2TP packet.
  - Data encryption begins before the PPP connection process by negotiating an IPSec security association.
  - Require computer-level authentication using computer certificates.

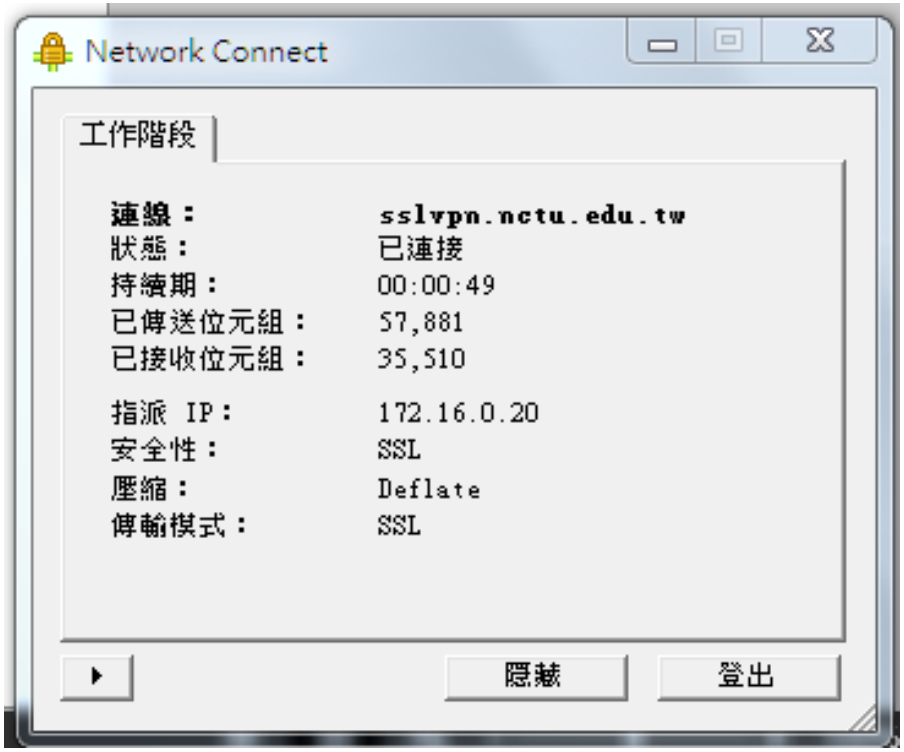


IPsec Tunnel Mode

- Internet Protocol Security Tunnel Mode
  - IPSec tunnel mode encapsulates and encrypts entire IP packets, and the encrypted payload is then encapsulated again with a plain-text IP header.
- Internet Key Exchange (IKE)
  - ISAKMP+OAKLEY
- Two functions that ensure confidentiality:
  - Authentication Header (AH)
    - Provide source authentication and integrity without encryption.
  - Encapsulating Security Payload (ESP)
    - Provide both data authentication, data integrity and data encryption.

SSL VPN

- A form of VPN that can be used with a standard Web browser.
- The traffic is encrypted with the SSL protocol or Transport Layer Security (TLS) protocol.



Appendix

- Seven Myths about VPN Logging and Anonymity
- https://technet.microsoft.com/zh-tw/library/bb742566.aspx