Security +
VPN Security

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

VPN

- Allows secure access of private network over public network
- Tunnelling protocols allow encapsulation and encryption of traffic to help protect confidentiality
- **Site-to-site VPNs** are used for corporate networks that span WAN (Wide area networks) in contrast to the normal VPN which is called **host-to-gateway model**
- **Always on VPN** defines a host-to-gateway model or site-to-site model VPN that is always functioning
- An **On-demand** or **Split tunnel VPN** defines a host-to-gateway or site-to-site model VPN that is only established when the user connects to a particular remote network resource

VPN Concentrator

- Dedicated devices that can support many clients and **isolate VPN authentication** and network access traffic
- They are commonly found in the DMZ

VDI Virtual Desktop Infrastructure

- Allows users to access workstation desktop resources using a mobile device

IPsec as a tunnelling protocol encrypts data in transit

- **Split tunnel**
  - Only encrypts traffic going to private IP addresses on the private network
  - All regular internet traffic is accessed directly through the gateway not via the VPN connection
- **Full tunnel**
  - All traffic from the client is encrypted and send over the VPN to be processed by the private network
  - This can ensure that all network traffic coming in and out of the client is filtered through the **UTM (unified thread management)** device
  - This ensures more security for corporate devices that are used in the field using public networks such as hotels, public wifi, other corporate networks, etc.
- **Transport Mode**
  - Only encrypts the data payload of the packet
  - Used in private networks, but not VPNs
- **Tunnel Mode**
  - Encrypts the entire IP packet
  - Used for VPN traffic that passes over internet

    - The remote internal routing IP address of the packets are encrypted
- **IPsec VPNs** use **authentication headers** (AH protocol number 51) to provide authentication and integrity, and **Encapsulating Security Payload** (ESP protocol 50) to encrypt the payload and provide confidentiality
- **IPsec VPNs** use **IKE Internet Key Exchange** on **port 500** to authenticate clients (RFC 2408)
- **IPsec** also uses **security associations (SAs)** to create a secure authenticated channel

SSTP Secure socket tunnelling protocol can be used when IPsec is not feasible

- SSTP is a proprietary **Microsoft** VPN protocol
- Transports **PPP** traffic through an **SSL/TLS** channel
- Operates over **TCP port 443** so it can pass through complex firewalls more easily since port 443 is usually open to allow encrypted web-traffic