References and Reading

This section includes the following references for further information:

- Documents:
  - IPsec VPN WAN Design Overview—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html
  - IPsec Direct Encapsulation Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Dir_Encap.html
  - Dynamic Multipoint VPN (DMVPN) Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG.html
  - Voice and Video Enabled IPsec VPN (V3PN) Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN_SRND.html
  - Multicast over IPsec VPN Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc.html
  - V3PN: Redundancy and Load Balancing Design Guide—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/VPNLoad/VPN_Load.html
  - Digital Certificates/PKI for IPsec VPNs—http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/DCertPKI.html
  - Enterprise QoS SRND—http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html
- Request For Comment (RFC) papers:
  - Security Architecture for the Internet Protocol—RFC2401
  - IP Authentication Header—RFC2402
  - The Use of HMAC-MD5-96 within ESP and AH—RFC2403
  - The Use of HMAC-SHA-1-96 within ESP and AH—RFC2404
  - The ESP DES-CBC Cipher Algorithm With Explicit IV—RFC2405
  - IP Encapsulating Security Payload (ESP)—RFC2406
  - The Internet IP Security Domain of Interpretation for ISAKMP—RFC2407
  - Internet and Key Management Protocol (ISAKMP)—RFC2408
  - The Internet Key Exchange (IKE)—RFC2409

- The NULL Encryption Algorithm and Its Use With IPsec—RFC2410
- IP Security Document Roadmap—RFC2411
- The OAKLEY Key Determination Protocol—RFC2412