Implementing Secure Solutions with Virtual Private Networks v1.0 (300-730)

Exam Description: Implementing Secure Solutions with Virtual Private Networks v1.0 (SVPN 300-730) is a 90-minute exam associated with the CCNP Security Certification. This exam tests a candidate's knowledge of implementing secure remote communications with Virtual Private Network (VPN) solutions including secure communications, architectures, and troubleshooting. The course, Implementing Secure Solutions with Virtual Private Networks, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

15%	**1.0**	**Site-to-site Virtual Private Networks on Routers and Firewalls**
	1.1	Describe GETVPN
	1.2	Implement DMVPN (hub-and-spoke and spoke-to-spoke on both IPv4 & IPv6)
	1.3	Implement FlexVPN (hub-and-spoke on both IPv4 & IPv6) using local AAA
20%	**2.0**	**Remote access VPNs**
	2.1	Implement AnyConnect IKEv2 VPNs on ASA and routers
	2.2	Implement AnyConnect SSLVPN on ASA and routers
	2.3	Implement Clientless SSLVPN on ASA and routers
	2.4	Implement Flex VPN on routers
35%	**3.0**	**Troubleshooting using ASDM and CLI**
	3.1	Troubleshoot IPsec
	3.2	Troubleshoot DMVPN
	3.3	Troubleshoot FlexVPN
	3.4	Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers
	3.5	Troubleshoot Clientless SSLVPN on ASA and routers
30%	**4.0**	**Secure Communications Architectures**
	4.1	Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
	4.2	Identify functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions
	4.3	Identify VPN technology based on configuration output for site-to-site VPN solutions
	4.4	Identify VPN technology based on configuration output for remote access VPN solutions
	4.5	Identify split tunneling requirements for remote access VPN solutions
	4.6	Design site-to-site VPN solutions
		4.6.a VPN technology considerations based on functional requirements
		4.6.b High availability considerations

4.7 Design remote access VPN solutions
- 4.7.a VPN technology considerations based on functional requirements
- 4.7.b High availability considerations
- 4.7.c Clientless SSL browser and client considerations and requirements

4.8 Identify Elliptic Curve Cryptography (ECC) algorithms