Cisco Security Architecture for System Engineers (700-765)

Exam Description:

The Security Architecture for Systems Engineers (SASE 700-765) is a 90-minute exam for the required knowledge across the Cisco Security portfolio for a registered partner organization to obtain the Security specialization in the SE role.

Exam Topics:

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. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

20%	**1.0**	**Threat Landscape and Security Issues**
	1.1	Identify the role of digitization in cyber security
	1.2	Identify key cyber security challenges
	1.3	Identify causes of fragmented security
	1.4	Identify security opportunities and obstacles
10%	**2.0**	**IoT Security**
	2.1	Identify IoT solutions critical to business
	2.2	Identify the evolution of and need for IoT security
	2.3	Identify how Cisco IoT Security solutions provide layered protection
	2.4	Identify components of Cisco's IoT security
10%	**3.0**	**Cisco Zero Trust**
	3.1	Identify the value of and drivers for trust-centric security
	3.2	Identify the value of zero trust
	3.3	Identify zero-trust solutions
	3.4	Identify Cisco Zero Trust outcomes
20%	**4.0**	**Cisco Security Solutions Portfolio**
	4.1	Identify the requirements of modern network environments
	4.2	Identify Cisco solutions for next generation network security
	4.3	Identify the areas of next generation network security
	4.4	Identify solutions for Web and Email Security
	4.5	Identify the elements of DNS-Layer Security
	4.6	Identify solutions for Cloud Security
	4.7	Identify the elements of Cloud-Delivered Security
10%	**5.0**	**Network Security**
	5.1	Identify solutions for NGFW and NGIPS
	5.2	Identify the elements of ASA

5.3   Identify features of Cisco Firepower Threat Defense
5.4   Identify features and management of Meraki MX

15%   6.0   Visibility and Enforcement
6.1   Identify solutions for Visibility and Enforcement
6.2   Identify the elements of AnyConnect
6.3   Identify the elements of ISE
6.4   Identify the elements of TrustSec
6.5   Identify the elements of Duo

15%   7.0.   Advanced Threat
7.1   Identify solutions for Advanced Threat
7.2   Identify the elements of Advanced Malware Protection
7.3   Identify the elements of ThreatGrid
7.4   Identify the elements of Cognitive Intelligence
7.5   Identify the elements of Stealthwatch