303 - ASM TECHNOLOGY SPECIALIST
EXAM BLUEPRINT

ABOUT THE 303-ASM SPECIALIST EXAM.
The 303-ASM Specialist exam is required to achieve the ASM Technology Specialist certification.

The Technology Specialist certification for Application Security Manager (ASM), builds upon the BIG-IP Administrator certification. The Technology Specialist certification assures prospective employers that the candidate is fully qualified to design, implement, and maintain ASM, including advanced features. (This certification is based on v11 of the F5 products.)

WHAT IS THE 303-ASM TECHNOLOGY SPECIALIST EXAM BLUEPRINT?
F5 Certified Exam Blueprints list all the objectives an exam has to measure, much like a syllabus for the exam itself. The blueprint provides the detailed breakdown of the skills and knowledge a candidate should have to pass the exam. Blueprints can be used to identify areas for additional study, and are best used in conjunction with the Exam Study Guides.

PREREQUISITE:
F5 Certified BIG-IP Administrator (F5-CA)

CREDENTIAL AWARDED:
F5 Certified Technology Specialist, ASM

THIS EXAM IS BASED ON V11.3

303 - ASM TECHNOLOGY SPECIALIST
EXAM BLUEPRINT

F5 CERTIFIED TECHNOLOGY SPECIALIST

Section 1:	Assess security needs and choose an appropriate ASM policy	Cognitive Complexity
Objective 1.01	Explain the potential effects of common attacks on web applications	U/A
Examples	Summarize the OWASP top ten Describe how ASM addresses the OWASP top ten	
Objective 1.02	Explain how specific security policies mitigate various web application attacks	U/A
Objective 1.03	Determine which ASM mitigation is appropriate for a particular vulnerability	U/A
Example	Explain the purpose of vulnerability assessment tools	
Objective 1.04	Choose the appropriate policy features and granularity	U/A
Examples	Describe the relationship between security policy and application development Explain how specific security policies mitigate various web application attacks	
Objective 1.05	Determine the most appropriate deployment method for a given set of requirements	A/E
Examples	Determine the appropriate deployment method when a “canned” deployment method is not applicable Evaluate the implications of changes in the policy to the security and vulnerabilities of the application	
Objective 1.06	Evaluate the implications of changes in the policy to the security and vulnerabilities of the application	U/A
Examples	Determine rate of change of the application Explain the trade-offs between security, manageability, false positives, and performance	

Section 2:	Create and customize policies	Cognitive Complexity
Objective 2.01	Determine the appropriate criteria for initial policy definition based on application requirements (e.g., wildcards, violations, entities, signatures, user-defined signatures)	U/A
Example	Define the policy based on application requirements	
Objective 2.02	Explain the policy builder lifecycle	U/A
Objective 2.03	Review and evaluate rules based on information gathered from ASM (e.g., attack signatures, DataGuard, parameters, entities)	U/A

Cognitive Complexity Key:
R=Remember
A/E=Analyze/Evaluate
U/A=Understand/Apply

Objective 2.04	Refine policy structure for policy elements (e.g., URLs, parameters, files types, headers, sessions and logins, content profiles, CSRF protection, anomaly protection)	U/A
Objective 2.05	Explain the process to integrate and configure natively supported third-party vendors and generic formats with ASM (e.g., difference between scanning modes, iCAP)	U/A
Examples	Upload scan results from a third-party vendor into the ASM GUI	
Objective 2.06	Determine whether the rules are being implemented effectively and appropriately to mitigate the violations	U/A
Examples	Determine the appropriate violations to be enforced	
Objective 2.07	Explain reporting and remote logging capabilities	A/E
Examples	Determine whether the remote logger is accessible Determine the level of logging (i.e., all logs, illegal requests, or responses)	
Section 3:	**Maintain policy**	Cognitive Complexity
Objective 3.01	Interpret log entries to identify opportunities to refine the policy	R
Examples	Describe the various logs and formats Identify the current state of the policy (e.g., violation status, blocking mode)	
Objective 3.02	Determine how a policy should be adjusted based upon available data (e.g., learning suggestions, log data, application changes, traffic type, user requirements)	U/A
Examples	React to changes in the web application infrastructure Adjust the policy to address application changes	
Section 4:	**Administer and evaluate ASM implementation**	Cognitive Complexity
Objective 4.01	Describe the lifecycle of attack signatures	U/A
Objective 4.02	Evaluate the impact of new or updated attack signatures on existing security policies	U/A
Examples	Apply the changes and fixes to the system and/or policies	

Cognitive Complexity Key:
R=Remember
A/E=Analyze/Evaluate
U/A=Understand/Apply

Objective 4.03	Identify key ASM performance metrics (e.g., CPU report, memory report, process requests, logging)	U/A
Objective 4.04	Interpret ASM performance metrics and draw conclusions	R
Examples	Identify key ASM performance metrics Recognize ASM device limitations Identify sources of resources consumption (e.g., large file uploads)	
Objective 4.05	Identify and gather information relevant to evaluating the activity of an ASM implementation	U/A
Objective 4.06	Interpret the activity of an ASM implementation to determine its effectiveness	U/A
Examples	Demonstrate an understanding of the growth trajectories for appropriate on-going operations Appraise the ASM specific system resources (e.g., box capacity)	
Objective 4.07	Differentiate between blocking and transparent features	R
Examples	Recognize the components of a PCI compliance report Differentiate between blocking and transparent features	
Objective 4.08	Evaluate whether a security policy is performing per the requirements (i.e., blocking, transparent, or other relevant security features)	U/A
Examples	Solve issues that are illustrated in the PCI compliance report Recognize the importance of trends and communicate to the necessary stakeholders Explain risk management and the balance between availability and security	
Objective 4.09	Define the ASM policy management functions (e.g., auditing merging, reverting, import, export)	R
Examples	Describe how to export/import policies Explain how to merge and differentiate between policies Describe how to revert policies Review the policy log	
Objective 4.10	Explain the circumstances under which it is appropriate to use ASM bypass	R
Examples	Recognize ASM specific user roles Recognize differences between user roles/permissions	

Cognitive Complexity Key:
R=Remember
A/E=Analyze/Evaluate
U/A=Understand/Apply

Cognitive Complexity Descriptions

Lower Order Thinking Skills → Higher Order Thinking Skills

Remember	Understand/Apply	Analyze/Evaluate	Create
Information retrieval	Knowledge transfer	Critical thinking and reasoning	Innovation or Creative thinking
Rote memorization	Comprehension or Ability to apply knowledge to a standard process	Determine how parts relate to whole or Knowledge integration and application to new situation(s)	Forming an original work product
Retrieve relevant knowledge from long-term memory	Construct meaning from information	Make judgments based on criteria	Combine or reorganize parts to form a new pattern or structure
e.g., recall, retrieve, recognize	e.g., interpret, classify, compare, explain, implement	e.g., troubleshoot, attribute, diagnose, critique	e.g., generate, plan, produce

Alpine Testing Solutions' suggested cognitive complexity levels and associated verb references consider multiple approaches to defining cognitive processing (e.g., Anderson et al., Webb, Bloom, Frisbie). Above material created with assistance from Alpine and distributed with Alpine's permission as an attachment to certification test blueprints.

Alpine Testing Solutions

Alpine Testing Solutions, Inc. (Alpine) gives F5 Networks permission to distribute the PDF "Cognitive Complexity Description 20130418.pdf" as an attachment to certification test blueprints created with assistance from Alpine into the exam blueprint.