

Exam Code: F50-526

Exam Name: BIG-IP ASM 9.4.5

Vendor: F5 Networks

Version: DEMO

Part: A

1: Which method of protection is not provided by the Rapid Deployment policy template?

- A.Data leakage
- B.Buffer overflow
- C.HTTP protocol compliance
- D.Dynamic parameter validation

Correct Answers: D

2: Which of the following methods are used by the BIG-IP ASM System to protect against SQL injections?

- A.HTTP RFC compliancy checks
- B.Meta-character enforcement and attack signatures
- C.HTTP RFC compliancy checks and length restrictions
- D.Response scrubbing, HTTP RFC compliancy checks, and meta-character enforcement

Correct Answers: B

3: Which statement is correct concerning differences between BIG-IP ASM platforms?

- A.The 4100 has more ports than the 3600.
- B.The 4100 and 3600 have the same number of ports.
- C.The 4100 and 3600 can support both the module and standalone versions of BIG-IP ASM.
- D.The 4100 can support only the standalone version of BIG-IP ASM whereas the 3600 can support both module and standalone versions of BIG-IP ASM.

Correct Answers: D

4: A security audit has determined that your web application is vulnerable to a cross-site scripting attack. Which of the following measures are appropriate when building a security policy? (Choose 2)

- A.Cookie length must be restricted to 1024 bytes.
- B.Attack signature sets must be applied to any user input parameters.
- C.Parameter data entered for explicit objects must be checked for minimum and maximum values.
- D.Parameter data entered for flow-level parameters must allow some meta-characters but not others.

Correct Answers: B D

5: Which of the following is not a feature of a standalone BIG-IP ASM System?

- A.Attack signatures
- B.Multiple pool members
- C.Positive security model
- D.Real-time traffic policy builder
- E.Pre-defined security policy templates

Correct Answers: B

6: Which of the following can be associated with an XML profile?

- A.Flow
- B.Method
- C.Parameter
- D.Object type

Correct Answers: C

7: Which of the following is correct concerning HTTP classes?

- A.A single web application can be used by several HTTP classes
- B.A virtual server can only have one web application associated with it
- C.A single ASM enabled HTTP class can be used by multiple virtual servers
- D.Each ASM enabled HTTP class can have several active security policies associated with it

Correct Answers: C

8: A user is building a security policy using the Deployment Wizard and the QA lab deployment scenario. By default, which settings will be applied to the security policy? (Choose 2)

- A.The security template will be set to Typical.
- B.The default traffic source will be live traffic.
- C.The enforcement mode will be set to blocking.
- D.The encoding language will be set to auto detect.
- E.The Attack signatures applied to the security policy will be only user created signature sets.

Correct Answers: B D

9: The Heuristics process is designed to ensure what aspect of a good security policy?

- A.The response traffic is sampled by the policy builder.
- B.A security policy is built with a minimum amount of false positives.
- C.The security policy accurately reflects all elements of a web application.
- D.All possible parameter values are automatically configured in the security policy.

Correct Answers: B

10: When building a policy based on live traffic using the automated policy builder, which of the following elements will not be taken into account when analyzing the traffic?

- A.The size of the response
- B.The requested resource (URI)
- C.The response code from the web server
- D.The parameter values of static based parameters

Correct Answers: A

11: Which of the following statements are correct regarding positive and negative security models? (Choose 2)

- A.Positive security model allows all transactions by default.
- B.Negative security model denies all transactions by default.
- C.Negative security model allows all transactions by default and rejects only transactions that contain attacks.
- D.Positive security model denies all transactions by default and uses rules that allow only those

transactions that are considered safe and alid.

Correct Answers: C D

12: Which of the following are correct when using the Policy Builder with trusted traffic? (Choose 2)

- A.All request data observed by the BIG-IP ASM System will be applied to the active security policy
- B.The BIG-IP ASM System will build the security policy without using HTTP response data
- C.Heuristics will be used to determine if an entity becomes an element of an active security policy
- D.The BIG-IP ASM System will automatically scan the web application to look for security violations

Correct Answers: A B

13: Learning suggestions in the Policy Building pages allow for which of the following? (Choose 2)

- A.XML-based parameters and associated schema are automatically learned.
- B.Blocking response pages can be automatically generated from web site content.
- C.Flow level parameters are displayed when found and can be accepted into the current policy.
- D.The administrator may modify whether the BIG-IP ASM System will learn, alarm, or block detected violations.
- E.Maximum acceptable values for length violations are calculated and can be accepted into the security policy by the administrator.

Correct Answers: C E

14: Which of the following methods of protection is not available within the Protocol Security Manager for HTTP traffic?

- A.Data guard
- B.Attack signatures
- C.Evasion techniques
- D.Object type enforcement

Correct Answers: B

15: The Application Security Policy Editor user role can perform which of the following functions? (Choose 2)

- A.Modify HTTP class profiles
- B.Create new HTTP class profiles
- C.Create new Attack signature sets
- D.Assign HTTP class profiles to virtual servers
- E.Configure Advanced options within the BIG-IP ASM System

Correct Answers: C E