Vendor: IBM

Exam Code: 000-609

Exam Name: IBM WebSphere Datapower SOA Appliances Firmware V3.8.1, Solution Implementation

Version: DEMO

1. Which of the following is an advantage of using WS-Security instead of SSL?
A. Provides assured message delivery.
B. Provides message integrity for the entire message.
C. Provides security in end-to-end scenarios across trust boundaries.
D. Provides mutual authentication to authenticate both the server and client.
Answer: C

2. A customer would like to use a WebSphere DataPower service to translate inbound xml messages into COBOL copybook messages. The translation will be performed by a predefined WebSphere Transformation Extender map file. The DataPower service should support both WebSphere MQ and HTTP on the front-side. Based on the scenario above, which of the following is the MOST appropriate DataPower service type?
A. Web Service Proxy
B. XML Firewall Service
C. Multi-Protocol Gateway
D. Web Application Firewall
Answer: C

3. A company is planning to implement disaster recovery (DR) for their two existing WebSphere DataPower Integration Appliance XI50s which have been used for different projects.
The following conditions apply:
1) The two devices (source and target appliance) are located in geographically dispersed data centers.
2) The firmware level is V3.8.1 on the source appliance and V3.8.1 on the target appliance and their hardware is compatible
3) Both appliances have a different set of users that need to be merged
4) The source appliance has been initialized with disaster recovery mode and is to be securely backed up and restored on to the target appliance.
Which of the following statements is TRUE and supports the above conditions?
A. The target appliance must be set to disaster recovery mode for the secure restore to be successful.
B. Merge the contents of the source appliance with the target appliance so as to merge the users on both appliances and do not use the overwrite option when prompted.
C. The target device will be overwritten. It is not possible to automatically merge the different users on source and target appliances using secure backup and restore.
D. After a secure restore was run, the administrator realizes that some existing data on the target appliance needs to be saved so the admin can stop the secure restore and start it later after backing up required data on the target appliance
Answer: C

4. A customer wants to protect communication between two WebSphere DataPower appliances against a replay attack. The second DataPower appliance needs to validate

that the messages received from the first appliance have spent no more than 30 seconds in transit.
Which of the following configurations would meet these requirements?
A. Set the var://service/transaction-timeout variable on the first DataPower appliance to 30 seconds.
B. Configure mutually authenticated SSL between the two DataPower appliances with an SSL timeout configured to 30 seconds.
C. Configure the front side handler on the second DataPower appliance with the Stale Connection Timeout field set to 30 seconds.
D. Use a scheduled processing policy rule on the second DataPower appliance containing a Filter action and configured to run every 30 seconds.
E. Use symmetric encryption to encrypt a token containing a timestamp on the first DataPower appliance and decrypt it on the second appliance.
Answer: E

5. Which of the following protocols are NOT supported by Front Side Handlers?
A. FTP
B. NFS
C. RSS
D. IIOP
E. Tibco EMS
F. WebSphere MQ
Answer: CD

6. A customer would like to use a Multi-Protocol Gateway (MPGW) to process an inbound XML message and use a local XSL file to map some of its data to a SOAP message. When configuring the processing policy for this MPGW, which of the following actions should be used for the data mapping?
A. Transform (xform)
B. Transform PI (xformpi)
C. Transform Binary (xformbin)
D. Transform SOAP (xformsoap)
Answer: A

7. A solution implementer is debugging a Web Services Proxy with an HTTPS Front Side Handler listening on port 443. On the backend it communicates with a service http://server1:9092/myserv. The irregular performance to the backend service cannot be explained so a packet capture is run to dig deeper into the issue. The results need to be stored in a file called capture-1. Also the developer does not want to have irrelevant data captured so as to focus on the problem at hand. A size limit of 30 minutes of capture time or 2.5 meg of total size of the data captured (which ever occurs first) needs to be imposed. Which of the following packet capture CLI commands is correct?
A. packet-capture local:///capture-1 30 2.5 "host server1 and src port=443"
B. packet-capture temporary:///capture-1 30 2.5 "host server1 src port=443"

C. packet-capture temporary:///capture-1 1800 2500 "host server1 and dst port=443"
D. packet-capture temporary:///capture-1 1800 2500 "host server1 and dst port=9092"
Answer: D

8. Which of the following is the correct CIDR notation for the IP Address below?
IP Address: 192.168.1.81
Subnet Mask: 255.255.255.0
A. 192.168.1.81/8
B. 192.168.1.81/16
C. 192.168.1.81/24
D. 192.168.1.81/32
Answer: C
9. Which of the following IPv4 address classes supports a maximum of 256 addresses per subnet?
A. Class A
B. Class B
C. Class C
D. Class D
E. Class E
Answer: C

10. What is the size (in bytes) of an IPv6 IP address?
A. 4
B. 6
C. 8
D. 16
Answer: D

11. Which of the following IPv4 IP addresses is the loopback address?
A. 0.0.0.0
B. 0.0.0.1
C. 127.0.0.0
D. 127.0.0.1
E. 255.255.255.0
F. 255.255.255.1
Answer: D

12. A bank wants to use PKI so that its partners can securely access financial transaction data. Certificates signed by a well-known Certificate Authority are used to implement the solution.
Which of the following solution requirements match an appropriate field in the certificate?
A.
B.
C.

D.
E.
F.
Answer: AC

13. The SAML Holder of Key (HOK) method uses PKI to establish trust between a consumer and provider in different trust domains. An Attesting Entity that is trusted by both the consumer and the provider is used.
Here is an example of an HOK scenario:
1) A SOAP message is sent by a client to an Attesting Entity over SSL.
2) The Attesting Entity obtains the public key of the client and places it in the SAML token it is creating in response to the client request, and digitally signs the token.
3) The client adds that SAML token to the SOAP header and constructs the SOAP body, signs it with its own key, and calls the web service provider over SSL.
4) The web service provider verifies the SAML token was signed by the trusted Attesting Entity and processes the message.
Given this scenario, which of the following elements of PKI are used to establish trust between the consumer and provider?
A. The Attesting Entity, provider and consumer use a shared private key to establish trust between them.
B. The Attesting Entity sends its public key to the provider which the provider compares to the trusted public key in its key store to establish trust.
C. The Attesting Entity digitally signs the consumer message with its private key which the provider verifies using the trusted public key of the Attesting Entity.
D. The Attesting Entity vouches for the consumer since it authenticated the consumer first and asserts that by sending a SAML token to the provider over a secure channel.
Answer: C

14. Which of the following is NOT a required feature of a secure SSL connection?
A. Message integrity.
B. The negotiation of a shared secret key is secure.
C. The client credentials must be sent to the server.
D. The peer's identity can be authenticated using asymmetric, or public key cryptography.
Answer: C

15. SSL uses which encryption type to create a session between client and server?
A. Private Key encryption
B. Symmetric encryption
C. Asymmetric encryption
D. Both Symmetric and Asymmetric encryption
Answer: D