IBM 000-530

000-530 IBM Internet Security Systems Technical Test v1

Practice Test

Version 1.1

QUESTION NO: 1

A client requests a GX5108CF demonstration. After receiving the GX5108CF and BYP-2T-2S-0LP bypass unit, the client calls the SE and explains that the four segments in the network are copper running at 1GBPS. How should the SE respond?

A. Arrange for 2x (DUAL-TVR-KIT-TX-ROHS) transceiver kits and 1x (BYP-4T-0S-0L-P) bypass units.
B. Arrange for a Gx5108SFP with 4x (DUAL-TVR-KIT-LX-ROHS) transceiver kits.
C. Arrange for 4x (DUAL-TVR-KIT-TX-ROHS) transceiver kits (2 kits for NIPS and 2 kits for the bypass unit).
D. Arrange for 4x (DUAL-TVR-KIT-TX-ROHS) transceiver kits and 1x (BYP-4T-0S-0L-P) bypass units.

Answer: A

QUESTION NO: 2

An SE is accompanying the sales team to a sales presentation. The sales team asks the SE to discuss commercial and open-source vulnerability scanning solutions. What content should the SE include?

A. Vulnerability scanning tools must be based on high-quality vulnerability research to be most effective.
B. Commercial tools always check for more vulnerabilities than open source tools.
C. Open source tools might cause a denial of service during a scan, but commercial products never cause this problem.
D. Commercial vulnerability scanning tools are faster than open source tools.

Answer: A

QUESTION NO: 3

What would happen to traffic that matched a Proventia Network IPS Firewall rule with the action Protect?

A. It would be dropped.
B. It would go through the IDS signature policy.
C. It would trigger alerts only and never be blocked.
D. It would trigger a DNS lookup for the source IP address.

Answer: B

QUESTION NO: 4

In general, a SiteProtector appliance would not be suitable for which type of environment?

A. LargeEnterprise
B. Small Office
C. High Alert Volume
D. Distributed

Answer: B

QUESTION NO: 5

The X-Force research and development team is primarily concerned with which of the following?

A. Exploits discovered on the internet
B. Contracted research
C. Vulnerability research at IBM ISS
D. SNORT IDS signature standards

Answer: C

QUESTION NO: 6

What should the SE include as part of a post-deployment plan?

A. A post-installation training session
B. A project sign-off lunch
C. An overview of the possible future direction of the project
D. The Account Executive takes care of all post-deployment issues

Answer: A

QUESTION NO: 7

Which of the following would be the most appropriate design for a client who requires intrusion detection for an active-active pair of network segments?

A. A singleProventia Network IPS appliance in passive monitoring mode

B. A pair ofProventia Network IPS appliances in HA protection mode
C. A pair ofProventia Network IPS appliances in HA protection mode with power-failure bypass units
D. A pair ofProventia Network IPS appliances in HA assessment mode

Answer: A

QUESTION NO: 8

Which of the following is the best high-level summary of ISS to present to a management-level audience?

A. ISS products include network IPS appliances, Multi-Function Security appliances, desktop and server protection, vulnerability assessment, andSiteProtector management.
B. ISS usesstateful deep-packet inspection and buffer overflow exploit prevention to provide zero-day exploit prevention.
C. ISS uniquely combines security research, product development, and managed security services to deliver the optimum combination of cost effectiveness and pre-emptive protection.
D. ISS provides all the capabilities in the Network, Server, and Endpoint component of the IBM Security Framework.

Answer: C

QUESTION NO: 9

An SE is helping the sales team determine which Proventia Multi-Function Security appliance is the best fit for a client with a maximum of 2,250 users on a 100Mb/sec network segment. Which MFS model should the SE recommend?

A. MX1004
B. MX3006
C. MX5008
D. MX5110

Answer: D

QUESTION NO: 10

During a pre-sales presentation, the client asks the SE to create a basic cost benefit analysis. What should the SE do?

A. Use the partner pricing guide to define the project costs.
B. Include pricing in the presentation.
C. Work with the Account Executive to define the costs.
D. Include pricing in the presentation but explain that the costs may change.

Answer: C

QUESTION NO: 11

PCI compliance is associated with which industry?

A. Healthcare
B. Public Schools
C. Credit Card Processors
D. Stock Exchange

Answer: C

QUESTION NO: 12

What is needed to deploy a Proventia Network IPS in Passive Monitoring mode?

A. Cross-over cable
B. Firewall
C. Separate VLAN
D. Span or mirror port on a switch

Answer: D

QUESTION NO: 13

Which of the following is true regarding how SiteProtector can be deployed?

A. It can only be deployed as a stand-alone server or as an appliance.
B. It can be deployed in a stand-alone or distributed architecture.
C. It must be deployed by IBM ISS Professional Services.
D. It must be deployed with all Network IPS appliances.

Answer: B

QUESTION NO: 14

An SE must enter the IP address of whic component when connecting the Console to SiteProtector?

A. Application Server
B. Database
C. Event Collector
D. NearestSiteProtector Peer

Answer: A

QUESTION NO: 15

Which statement best describes the difference between the Host IPS engine in Proventia Desktop and the Network IPS engine in Proventia GX?

A. The Proventia Desktop and Proventia Network IPS engines perform the different checks.
B. The Proventia Desktop engine inspects traffic inside SSL encrypted sessions, and the Proventia Network IPS engine inspects traffic outside the sessions.
C. The Proventia Network IPS engine provides more granular policy management than the Proventia Desktop engine.
D. The Proventia Network IPS engine has a firewall policy and Proventia Desktop does not.

Answer: C

QUESTION NO: 16

What is a directory traversal exploit?

A. Traversing out of an application directory to system executables
B. Pushing code to a separate directory from the host application
C. Moving directories from one host to a less secure host
D. Using time zone differences to exploit code in a directory

Answer: A

QUESTION NO: 17

During a presentation, the sales team and SE learn that the client has finished evaluating three competing network IPS products. The client has to make a decision in two days. Which approach is the most appropriate?

A. Quickly determine evaluation criteria and provide the client with the comprehensive NSS report on IBM ISS appliances, highlighting the differentiators.
B. Persuade the client to perform a one-day evaluation of the IBM ISS product and to obtainMetasploit and Core Impact licenses for the process.
C. Offer the client X-Force services to hack the other three network IPS products and help with the evaluation.
D. Offer the client a Client Security Readiness Workshop which covers the IBM Information Security Framework.

Answer: A

QUESTION NO: 18

A client requests solutions for production and disaster recovery sites. The client has provided the network structure for the production site. When presenting IBM ISS solutions, which of the following is the next step in fulfilling the clients request?

A. Request a network diagram and detailed information about the disaster recovery site to determine further requirements.
B. Recommend the client purchase separate licenses and products for each site and design the solution based on the production site.
C. Recommend the client focus on protecting the production site because the disaster recovery site is a backup site.
D. Request the client install network IPS in the production site and host IPS in the disaster recovery Site.

Answer: A

QUESTION NO: 19

After initial meetings and follow-up discussions regarding IBM ISS offerings, a client requests a Proventia Server demonstration on the clients network. What is the SEs next step?

A. Ask the client for the network throughput, the link speeds, and the IP address for the SiteProtector appliance.
B. Invite the client to an informal, offsite meeting to discuss requirements for the demonstration and test.
C. Send the client a checklist of items to have ready, including the supported operating systems and kernel versions, the recommended memory and hardware requirements, and the IP address for theSiteProtector appliance.
D. Ask the client to testProventia Network IPS rather than Proventia Server because the Network IPS protects more servers than Proventia Server

Answer: C

QUESTION NO: 20

Which of the following tasks is most important in preparing an Enterprise Scanner demonstration?

A. Understand theclients current vulnerability management process and demonstrate benefits linked to the clients objective.
B. Boot up the appliance, ensure One Trust License works, and perform a test scan.
C. Have a working VMware version of the scanner as a backup.
D. Practice the demonstration in theclients environment a week in advance to build confidence and resolve issues.

Answer: A

QUESTION NO: 21

After an SE performs a successful Proventia Network IPS demonstration, the client requests a one-month evaluation period. How should the SE respond?

A. Obtainan Proventia Network IPS appliance and license.
Immediately send the appliance and license to the client.
Ensure the client can log in to support and submit inquiries.
B. Obtainan Proventia Network IPS appliance and license.
Deliver the Proventia Network IPS appliance and the license.
Avoid contacting the client or asking questions during the evaluation.
C. Schedule a time to go onsite for the evaluation.
Obtain an Proventia Network IPS appliance and license.
Conduct the evaluation and send a report to the client summarizing findings.
D. Schedule the evaluation at a time when there is a dedicated client resource.
Help the client create a list of evaluation items.
Call the client regularly during the evaluation to check progress and offer assistance.

Answer: D

QUESTION NO: 22

An SE is preparing a product demonstration for a client who is interested in

A. Propose a free health scan so the client can evaluate the Vulnerability Management Service as a MSS offering.

B. Determine the number of machines in the clients network, select the appropriateEnterprise Scanner model, and verify One Trust Licensing works for the appliance.
C. Propose an Internet Scanner demonstration and ensure an unlimited license is provided for the demo.
D. Discuss needs and requirements with the client and then propose either a Vulnerability Management Service or an Enterprise Scanner demonstration.

Answer: D

QUESTION NO: 23

An SE is preparing a Proventia Network IPS and SiteProtector demonstration for a client who is specifically concerned about daily operational efficiency, ease of use, and policy access control. Which tasks best demonstrate these features?

A. Enable X-Force recommended signatures and configure user permissions.
B. Decrypt SSL traffic for inspection and run a scan.
C. Define Open signatures and configure BOEP.
D. RunSecureSync and upload a One Trust License.

Answer: A

QUESTION NO: 24

Which component commits IDS events to the SiteProtector Database?

A. IDS Appliance
B. Agent Manager
C. Event Collector
D. Secure Sync

Answer: C

QUESTION NO: 25

A bank client is seeking protection against worms, viruses, and attacks. It has 100 remote branches that are linked to the Internet with no onsite technical expertise. Many of the branches are in rural areas without proper road access. The client wants to minimize any possible downtime. What products and features should an SE present to this customer?

A. PCI certifiedProventia MX0804 at remote branches, as it offers firewall protection, VPN, web filtering, mail filtering, and intrusion prevention system