JN0-541 Q&As

IDP, Associate(JNCIA-IDP)

Pass Juniper JN0-541 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/jn0-541.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

How do you access the ACM interface on an IDP sensor?

A. https://

B. http://

C. use the IDP user interface

D. use the SSH interface

Correct Answer: A

QUESTION 2

You want Enterprise Security Profiler (ESP) to capture layer 7 data of packets traversing the network. Which two steps must you perform? (Choose two.)

A. Configure ESP to enable application profiling, and select the contexts to profile.

B. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.

C. Start or restart the profiler process.

D. Create a filter in the ESP to show only tracked hosts.

Correct Answer: AC

QUESTION 3

What two statements are true about the Attack Object update process? (Choose two.)

A. The Attack Update must be manually downloaded by the administrator from the Juniper site and installed on each IDP S ensor.

B. The administrator is given the choice of which Dynamic Groups to update.

C. Attacks objects are downloaded from the Juniper site over TCP/443 (SSL) from the IDP User Interface.

D. A list of new, updated and removed attacks objects are displayed to the administrator.

Correct Answer: CD

QUESTION 4

Which method of detection does IDP Sensor use to detect an invalid IP address entering an external interface?

A. Layer2 Detection

B. DOS Detection

C. Spoofing Detection

D. Backdoor Detection

Correct Answer: C

QUESTION 5

What is the function of an IP action?

A. modifies the IP Header to prevent the attack

B. modifies the IP Header to redirect the attack

C. permits or denies the traffic, based on the IP Header

D. blocks subsequent connections from specific IP addresses

Correct Answer: D

QUESTION 6

Which three actions must be taken prior to deploying an IDP sensor (in transparent mode) in a network?

A. Assign an IP to the management interface IP.

B. Establish communication between Security manager and the sensor.

C. Assign an IP to all forwarding interfaces.

D. Configure the sensor mode.

Correct Answer: ABD

QUESTION 7

You have a rule in your IDP policy that detects all HTTP signatures that are targeted towards your Web server. You notice a log message is generated each time a Web user accesses the SQL database with the default passwords. Your Webmaster does not want to reprogram the Web page to use more secure SQL passwords. How do you disable alerts on this false positive?

A. Create a rule in the Exempt rule base; specify target address of your Web server; include only the specific HTTP SQL default password signature.

B. Create a rule at the top of the Exempt rule base; specify target address of your Web server; include all HTTP signatures.

C. Create a rule at the top of the IDP rule base for any traffic destined to your Web server; specify action of Exempt.

D. Create a rule at the top of the Exempt rule base; specify target address of your Web server; include all HTTP signatures; make this a terminal rule.

Correct Answer: A

QUESTION 8

Which account do you use to login when connecting to a sensor using SSL?

A. super

B. netscreen

C. admin

D. root

Correct Answer: D

QUESTION 9

Which three types of charts can be used in reports? (Choose three.)

A. vertical bar chart

B. line chart

C. pie chart

D. histogram

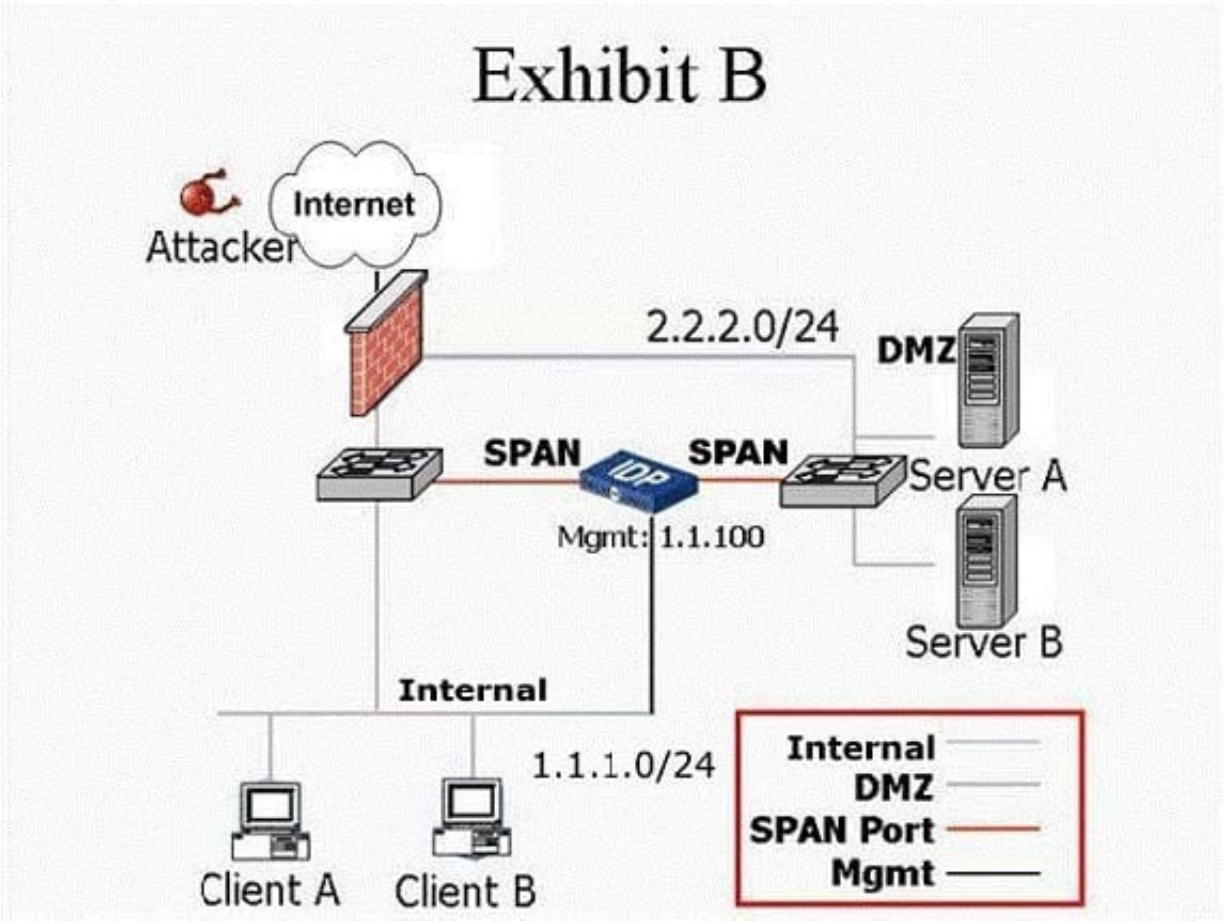
Correct Answer: ABC

QUESTION 10

Exhibit:

You work as an administrator at Certkiller .com. Study the exhibit carefully. Which three statements are true about the capabilities of IDP when deployed as shown in the exhibit? (Choose three.)

Exhibit:



A. IDP Sensor can detect attacks between Client A and Server A in this mode.

B. IDP Sensor can detect attacks between Server A and Server B in this mode.

C. IDP Sensor can only drop offending TCP traffic by sending TCP Resets in this mode.

D. IDP can drop any offending traffic between internal and DMZ networks in this mode.

Correct Answer: ABC

QUESTION 11

After you enable alerts for new hosts that are detected by the Enterprise Security Profiler, where do you look in Security Manager to see those alerts?

A. Security Monitor > Profiler > Application Profiler tab

B. Security Monitor > Profiler > Violation Viewer tab

C. Security Monitor > Profiler > Network Profiler tab

D. Log Viewer > Profiler Log

Correct Answer: D

QUESTION 12

Which statement is true about the NetScreen IDP Closed Loop Investigation (CLI)?

A. CLI describes the IDP Sensor command line utilities.

B. CLI provides easy navigation between Log Viewer and Log Investigator.

C. CLI provides easy navigation between Log Investigator, Log Viewer, Profiler information and quick reports.

D. CLI provides easy navigation between Log Investigator, Log Viewer, Profiler information and pre-defined reports.

Correct Answer: D

QUESTION 13

What are the limitations of using TCP Reset to block connections in an IDS? (Choose three.)

A. only works on TCP traffic

B. must know the correct packet size to successfully reset a connection

C. does not reset the connection until the attack has already taken place

D. resets all connections from a certain source-IP, which could lead to denial-of-service

Correct Answer: ACD

QUESTION 14

Which tool will allow you to change a sensor\\'s deployment mode?

A. ACM

B. ifconfig

C. sctop

D. Security Manager

Correct Answer: A

QUESTION 15

Which two tasks can be performed from the ACM? (Choose two.)

A. change the mode which IDP Sensor is operating

B. upgrade the firmware on the IDP Sensor

C. install a Security Policy on the IDP Sensor

D. change the Management IP address of a IDP Sensor

Correct Answer: AD