## Question: 1

Which statement is true about the attack object database update process?

A. Each sensor updates its own attack object database automatically; however they must be able to access the Juniper site on TCP port 443.
B. The attack object database update must be manually performed by the administrator, and the administrator must manually install it on each sensor.
C. The attack object database update can be initiated manually or automatically.
D. The attack object database update can be automatically scheduled to occur using the Security Manager GUI.

**Answer: C**

## Question: 2

On a sensor, which command will indicate if log messages are being sent to Security Manager?

A. scio vr list
B. service idp status
C. scio agentstats display
D. scio getsystem

**Answer: C**

## Question: 3

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

**Answer: D**

## Question: 4

When connecting to a sensor using SSH, which account do you use to login?

A. admin
B. super
C. netscreen
D. root

**Answer: A**

## Question: 5

Which OSI layer(s) of a packet does the IDP sensor examine?

A. layers 2-7
B. layers 2-4
C. layer 7 only
D. layers 4-7

**Answer: A**

## Question: 6

Which two will change the management IP of an IDP sensor? (Choose two.)

A. Edit the existing IDP sensor object in Security Manager GUI and change the IP address.
B. Delete the IDP sensor object from Security Manager and re-add the sensor with the new IP address.
C. Use ifconfig to change the management IP address.
D. Use the ACM to change the management IP address.

**Answer: B, D**

## Question: 7

Which rule base would detect netcat?

A. SYN protector
B. traffic anomalies
C. backdoor
D. exempt

**Answer: C**

## Question: 8

Which three fields in a packet must match an IDP rule before that packet is examined for an attack? (Choose three.)

A. terminate match
B. service
C. destination address

D. source address
E. attack object

**Answer: B, C, D**

## Question: 9

What is "a deviation from a protocol's expected behavior or packet format"?

A. context
B. compound attack object
C. attack signature
D. protocol anomaly

**Answer: D**

## Question: 10

A newly re-imaged sensor is running IDP 4.0 code. You want to assign IP address: 10.1.1.1 to the sensor. Which method do you use to do this?

A. Connect to the sensor's console port, login as root, and answer the EasyConfig
B. Use SSH to connect to the sensor at IP 192.168.1.1. Login as root, and run ipconfig.
C. Connect to the sensor's console port, login as admin, and answer the EasyConfig
D. Use SSH to connect to the sensor at IP 192.168.1.1. Login as admin, and run ipconfig.

**Answer: A**