

**Exam : Juniper JN0-541**

**Title : Juniper IDP,  
Associate(JNCIA-IDP)**

**Version : Demo**

## Important Note, Please Read Carefully

### Other VisualExams products

[All visual exams IT Exam Products](#)

### Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[visual exams Testing Engine](#)

### Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at VisualExams and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.visual exams.com/>
2. Log in the **User Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

### Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

Feedback should be send to [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com). You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

### Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com).

### Features

- Comprehensive questions with complete details
- Instant Downloadable in PDF form.
- Verified Answers Researched by Industry Experts
- Questions accompanied by exhibits.
- Drag and Drop questions as experienced in the Actual Exams.
- These questions and answers are backed by our GUARANTEE.
- Questions updated on regular basis.
- Like actual certification exams our product is in multiple-choice questions (MCQs)

**Commitment to Your Success: At VisualTestExam.com, we are committed to your ongoing success. Our exams and questions are constantly being updated and compared to industry standards.**

Want to earn a Microsoft certification like MCSE, MCSE 2003, CCNA, CCNP? Thinking about getting an A+ or CCSP?

A, CCSP or Network+ Certification with less effort and time. You will be astonished at the theoretical and practical knowledge you will acquire in such a short period of time using our Certification Training Products. Our Study material will enable you to pass your Microsoft, Your Cisco and any other certification on the very first attempt.

## **Guarantee**

VisualExams provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if somehow you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

**Answer: C**

2. You implement Traffic Anomaly detection and you find numerous alerts of port scans from your security auditing team that you want to ignore. You create an address book entry for the security audit team specifying the IP addresses of those machines.

What should you do next?

- A. Create a rule at the top of the Traffic Anomaly rulebase to ignore traffic from security audit team.
- B. Create an exempt rule for the security audit team in the Exempt rulebase to ignore Traffic Anomalies.
- C. Create a rule at the top of the IDP rulebase to ignore traffic from security audit team, and make this a terminal rule.
- D. Create a rule at the top of the Traffic Anomaly rule base to ignore traffic from security audit team, and make this a terminal rule.

**Answer: A**

3. You want Enterprise Security Profiler (ESP) to generate a message when a new host is detected on a network.

Which two steps must you perform? (Choose two.)

- A. Start or restart the profiler process.
- B. Configure ESP to enable alerts for new host detected.
- C. Configure ESP to enable application profiling, and select the contexts to profile.
- D. Under the Violation Viewer tab, create a permitted object, select that object, and then click Apply.

**Answer: AB**

4. Click the Exhibit button.

Source-IP	Port	Destination-IP	Port	Flag	Dir	State	Service	Timeout
10.1.1.50	32875	10.1.1.100	21	R---	-->	Estb	-	3597/3600
10.1.1.100	21	10.1.1.50	32875	R---	-->	Estb	-	3597/3600
10.1.1.50	32877	10.1.1.100	1645	R---	-->	GAWAY	-	2/5
10.1.1.100	1645	10.1.1.50	32877	R---	-->	GAWAY	-	2/5

In the exhibit, which sensor command would have produced this display?

- A. sctop "t" option
- B. sctop "s" option
- C. scio policy list s0
- D. scio subs qmodules s0

**Answer: A**

5. In which three situations would you create a compound attack object? (Choose three.)

- A. When attack objects must occur in a particular order.
- B. When one of the attack objects is a protocol anomaly.
- C. You have at least two attack objects that define a single attack.
- D. When the pattern needs to be defined using a stream 256 context.
- E. When the pattern "@@@" and context "ftp-get-filename" completely define the attack.

**Answer: ABC**

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

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

**Answer: B**

7. If the power is lost to an IDP sensor, which feature allows the traffic to continue to flow through the device?

- A. NIC bypass
- B. stateful inspection
- C. peer port modulation
- D. protocol anomaly detection

**Answer: A**

8. Which three functions does the IDP sensor perform? (Choose three.)

- A. detects new hosts on the network
- B. displays logs in Security Manager GUI
- C. performs attack detection and prevention
- D. forwards logs and status messages to Security Manager server

**Answer: ACD**

9. Which interface does IDP use to communicate with Security Manager?

- A. eth0
- B. eth1
- C. HA port
- D. console port

**Answer: A**

10. Which TCP port is used for communication between ACM and an IDP sensor?

- A. 80
- B. 443
- C. 7800
- D. 7801

**Answer: B**

11. Which TCP port is used for communication between Security Manager and an IDP sensor?

- A. 443
- B. 7800
- C. 7801
- D. 7803

**Answer: D**

12. Which three statements are true as they relate to a transparent mode IDP deployment? (Choose three.)

- A. Can actively prevent attacks on all traffic.
- B. An IP address must be defined on each forwarding interface.
- C. Can be installed in the network without changing IP addresses or routes.
- D. Uses paired ports, such that packets arriving on one port go out the other associated port.

**Answer:** ACD

13. Which two statements are true as they relate to a sniffer mode IDP sensor deployment? (Choose two.)

- A. An IP address must be assigned to the sniffer interface.
- B. It does not affect the performance or availability of the network.
- C. It provides passive monitoring only with limited attack prevention.
- D. IDP sensor cannot be managed by Security Manager in sniffer mode. IDP sensor cannot be managed by Security Manager in sniffer mode.

**Answer:** BC

14. Given the following steps:

- a. Attach the sensor to the management network.
- b. Place the sensor inline in network.
- c. Create and install a policy on the sensor.
- d. Establish communication between Security Manager and the IDP sensor.
- e. Configure the sensor deployment mode and management interface IP.
- f. Test connectivity through the sensor.

Which order is correct when initially deploying a sensor in a network?

- A. a, e, d, c, f, b
- B. e, a, d, b, f, c
- C. e, a, d, c, b, f
- D. b, f, e, a, d, c

**Answer:** B

15. Which three are assigned as a result of running EasyConfig? (Choose three.)

- A. sensor default gateway
- B. sensor eth0 IP address
- C. sensor eth1 IP address
- D. sensor HA configuration
- E. sensor deployment mode

**Answer:** ABE

16. Which type of cable do you use for a console connection to an IDP sensor?

- A. CAT 5 cable
- B. null-modem cable
- C. Juniper proprietary cable
- D. straight-through serial cable

**Answer:** B

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

**Answer:** D

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

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

**Answer:** C

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

- A. Configure the sensor mode.
- B. Assign an IP to all forwarding interfaces.
- C. Assign an IP to the management interface IP.
- D. Establish communication between Security manager and the sensor.

**Answer:** ACD

20. What is the default admin account password on the sensor?

- A. admin
- B. abc123
- C. juniper01
- D. password

**Answer:** B

Visualexams.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially Adobe, Apple, Citrix, Comptia, EMC, HP, HuaWei, LPI, Nortel, Oracle, SUN, Vmware and so on. And help you pass any IT Certification exams at the first try.

Web site: <http://www.visualexams.com>

You can reach us at any of the email addresses listed below.

E-Mail: [visualexams \(at\) hotmail.Com](mailto:visualexams@hotmail.com)