



## [Juniper Networks jn0-540](#)

**Exam Name:** *juniper networks certified internet associate.idp(jncia-idp)*

**Q & A :** 115 Q&As

***Pdf Demo***

### **Quality and Value for the jn0-540 Exam**

[Just4Exams Practice Exams](#) for Juniper Networks JNCIA jn0-540 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

### **100% Guarantee to Pass Your jn0-540 Exam**

If you do not pass the JNCIA jn0-540 exam on your first attempt using our Just4Exams *jn0-540 testing engine and pdf study guide*, we will give you a FULL REFUND of your purchasing fee.

### **Downloadable, Interactive jn0-540 Testing engines and PDF Version**

Our Exam Preparation Material provides you everything you will need to take a [JNCIA certification](#) examination. Details are researched and produced by [Juniper Networks Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

**Free jn0-540 Exams:**

***This is demo only, this pdf do not include the questions and answers picture***

Exam : Juniper JN0-540

Title : Juniper Networks Certified Internet Associate.idp(jncia-idp)

1. Which two attack detection methods are unique to Juniper NetScreenIDP? (Choose two.)

- A.Protocol Anomaly
- B.Packet Signatures
- C.Statefull Signatures
- D.Backdoor Detection

Answer: CD

2. Which three statements are true about custom reports? (Choose three.)

- A.Log filters can be applied to custom reports.

- B.You can export custom reports to pdf format.
- C.All custom reports are stored on per user basis.
- D.Creating reports using indexed columns is significantly faster.

Answer: ACD

3. What is a buffer overflow attack?

- A.a misconfigured application that has a known security hole
- B.an attack that overflows a server with many connections until it crashes
- C.an attack that takes advantage of a backdoor within a vulnerable application
- D.an attack which injects just the right amount of data into a vulnerable application, causing the application to execute the malicious code that was injected

Answer: D

4. Which statements are true about the IDP Management Server? (Choose two.)

- A.One IDP Management Server can manage multiple IDP Sensors.
- B.Each IDP Sensor must have its own Management Server component.
- C.The IDP Management Server process can be run on a IDP Sensor for evaluation purposes.
- D.Supported operating systems for IDP Management Server are Windows 2000, BSD UNIX, and Linux.

Answer: AC

5. What best describes Reconnaissance attacks?

- A.transmission of TCP SYN requests from a spoofed IP address
- B.transmission of ping packets of certain size to crash a remote host
- C.unauthorized discovery and mapping of systems, services, or vulnerabilities
- D.disabling or corrupting networks, systems, or services with the intent to deny the service to intended users

Answer: C

6. Which IDP Sensor is recommended to support onboard Management Server?

- A.IDP-10
- B.IDP-100
- C.IDP-500
- D.IDP-1000

Answer: B

7. Which method of detection does IDP Sensor use to detect attacks against a fake system on the network?

- A.Network Honeypot
- B.Spoofing Detection
- C.Stateful Signatures
- D.Backdoor Detection

Answer: A

8. Which two statements about disk management on the IDP Sensor are true? (Choose two.)

- A.IDP Management Server can be configured to send disk space alerts.
- B.If the IDP Sensor disk is full, the IDP Sensor will not store any additional logs or packet captures.
- C.If the IDP Sensor disk is full IDP Sensor starts oldest log entries first, and packet captures second.
- D.If the IDP Management Server disk is full, the oldest packet captures are purged first, and the log messages are purged second.

Answer: AD

9. Which layers of the OSI Model does IDP look into when inspecting a packet?

- A.Layers 2-7
- B.Layers 3-7
- C.Layer 7 only
- D.Layers 2-4 only

Answer: A

10. Which three columns can be seen in the Application view of Profiler? (Choose three.)

- A.Protocol
- B.Context and Context Value
- C.Source and Destination IPs
- D.Date First Seen and Last Seen

Answer: BCD

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

- A. only works on TCP traffic
- B. does not reset the connection until the attack has already taken place
- C. must know the correct packet size to successfully reset a connection
- D. resets all connections from a certain source-IP, which could lead to denial-of-service

Answer: ABD

12. Which three best describe denial-of-service attacks? (Choose three.)

- A. transmission of ping packets of a certain size to crash a remote host
- B. the unauthorized discovery and mapping of systems, services, or vulnerabilities
- C. transmission of TCP SYN requests from a spoofed IP address to exhaust the resources of a victim
- D. disabling or corrupting networks, systems, or services with the intent to deny the service to intended users

Answer: ACD

13. Which two statements are true about Trojans? (Choose two.)

- A. They are executables that infect only executable programs.
- B. They are programs often used to gather information about a host.
- C. They can secretly permit access to an infected computer from an outside host.
- D. They are programs that target only web servers by overwhelming them with traffic.

Answer: BC

14. Which method of detection does IDP Sensor use to detect a network scan or portscan?

- A. DOS Detection
- B. Traffic Anomaly
- C. Protocol Anomaly
- D. Backdoor Detection

Answer: B

15. What is the function of the IDP User Interface?

- A. It stores Security Policies and Attack Objects
- B. It supplements the Command-Line Interface on the Sensor, but is not required.
- C. It downloads logs from various Sensors and displays them to the administrator.
- D. It provides an interface for the administrator to view Logs/Reports and define Security Policies.

Answer: D

16. What are two drawbacks of an IDS system blocking an IP address? (Choose two.)

- A. works only on TCP traffic
- B. might not block the attacker until the attack has already taken place
- C. need to know the sequence number of the attacker's IP Header to successfully block the IP address
- D. might lead to denial-of-service situation where attacker can intentionally block valid users from accessing a network

Answer: BD

17. Which three functions can the IDP Sensor perform? (Choose three.)

- A. performs attack detection and prevention
- B. collects and presents logs to the IDP User Interface
- C. forwards logs and status messages to the IDP Management Server
- D. store logs locally when the IDP Management Server is unreachable

Answer: ACD

18. What are two limitations of traditional IDS systems? (Choose two.)

- A. do not detect internal attacks
- B. do not use signatures for known attacks
- C. do not operate inline so they cannot effectively block all attacks
- D. frequently have false positives due to less accurate packet signatures

Answer: CD

19. What is a Close Server action?

- A. issues a TCP Reset to the server only
- B. drops all packets from the attacker's IP
- C. drops any packet matching this src/dst/protocol

D.drops only the specific packet matching the attack pattern

Answer: A

20. What are three functions of the IDP Management Server? (Choose three.)

A.blocks attacks

B.stores Security Policies and Attack Objects

C.consolidates logs from the various IDP Sensors in a network

D.receive and manages connections from IDP User Interfaces

Answer: BCD

More [jn0-540 Braindumps](#) Information

#### **Related jn0-540 Exams**

JN0-100	JN0-522	JN0-342	JN0-400	JN0-141
jn0-201	jn0-320	JN0-521	JN0-341	jn0-120
JN0-311	jn0-541	jn0-570	jn0-540	JN0-562
JN0-321	jn0-561	jn0-140	jn0-520	JN0-340

#### **Other Juniper Networks Exams**

jn0-201	JN0-562	JN0-532	jn0-530	JN0-321
jn0-130	JN0-340	jn0-303	JN0-311	JN0-331
JN0-341	JN0-141	jn0-310	JN0-342	jn0-140
JN0-100	JN0-400	jn0-540	jn0-320	jn0-531