

## 2B0-018 Enterasys Networks Certification Enterasys Networks ES Dragon IDS

**Practice Exam:** 2B0-018 Exams

**Exam Number/Code:** 2B0-018

**Exam Name:** ES Dragon IDS

**Questions and Answers:** 50 Q&As

( [Enterasys Networks Certification](#) )



Exam : [2B0-018](#)

"ES Dragon IDS", also known as 2B0-018 exam, is a Enterasys Networks certification. With the complete collection of questions and answers, TestInside has assembled to take you through 50 Q&As to your 2B0-018

Exam preparation. In the 2B0-018 exam resources, you will cover every field and category in Enterasys Networks Certification helping to ready you for your successful Enterasys Networks Certification.

Quality and Value for the 2B0-018 Exam TestInside Practice Exams for Enterasys Networks **Enterasys Networks Certification** Certification 2B0-018 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

### **TestInside provide the professional Q&A.**

1. We offer free update service for three month.

After you purchase our product, we will offer free update in time for three month.

2. High quality and Value for the 2B0-018 Exam.

2B0-018 simulation test questions, including the examination question and the answer, complete by our senior IT lecturers and the Enterasys Networks Certification product experts, included the current newest 2B0-018 examination questions.

3. 100% Guarantee to Pass Your Enterasys Networks Certification exam and get your Enterasys Networks Certification Certification.

If you do not pass the Enterasys Networks Certification 2B0-018 exam (ES Dragon IDS) on your first attempt using our TestInside testing engine and pdf file, we will give you a FULL REFUND of your purchasing fee.

### **use TestInside 2B0-018 Q&A ensure you pass the exam at your first try.**

TestInside professional provide Enterasys Networks Certification 2B0-018 the newest Q&A, completely covers 2B0-018 test original topic. With our complete Enterasys Networks Certification resources, you will minimize your Enterasys Networks Certification cost and be ready to pass your 2B0-018 tests on Your First Try, 100% Money Back Guarantee included!

[Enterasys Networks 2B0-018](#) Test belongs to one of the Enterasys Networks Certification certified test, if needs to obtain the Enterasys Networks Certification certificate, you also need to participate in other related test, the details you may visit the [Enterasys Networks Certification](#) certified topic, in there, you will see all related Enterasys Networks Certification certified subject of examination.

### **TestInside Testing Engine Features**

Comprehensive questions and answers about 2B0-018 exam

2B0-018 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

2B0-018 exam questions updated on regular basis

Same type as the certification exams, 2B0-018 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 2B0-018 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : Enterasys Networks 2B0-018

Title : ES Dragon IDS

1. For what purpose can Dragon Workbench be used?

- A. Read data from TCPDUMP trace/capture file and write to dragon.db for later analysis
- B. Read data from dragon.db file and write to a TCPDUMP trace/capture file for later analysis
- C. Read data from RealTime Console and write to a TCPDUMP trace/capture file for later analysis
- D. This functionality is ONLY available on Dragon Appliances

Answer: A

2. Which of the following is NOT a typical function of an Intrusion Detection System?

- A. Monitors segment traffic to detect suspicious activity
- B. Monitors network traffic and corrects attacks
- C. Monitors traffic patterns to report on malicious events
- D. Monitors individual hosts (HIDS) or network segments (NIDS)

Answer: B

3. Which best describes a type of attack that aims to prevent the use of a service or host?

- A. Reconnaissance
- B. Denial of Service
- C. IP Spoofing
- D. Exploit

Answer: B

4. What is the primary and default source of event data for Dragon RealTime Console?

- A. dragon.log.xxx
- B. dragon.db
- C. Ring Buffer
- D. Dragon Workbench

Answer: C

5. What is the method that Dragon uses to secure the communication between the remote management host and Dragon Policy Manager?

- A. SSH
- B. SSL
- C. IPSec
- D. MD5

Answer: B

6. Which of the following is NOT a recommended means for a Dragon Network Sensor to collect event data over multiple switched links?

- A. Port Redirection

- B. Network Tap(s)
- C. Port Trunking
- D. Strategic deployment of multiple Dragon Network Sensors

Answer: C

7. What is one method of de-activating a Dragon Policy Manager on a Linux host?

- A. `./dragonctl kill PolicyManager`
- B. `./dragonctl kill policy-manager`
- C. `./dragonctl stop PolicyManager`
- D. `./dragonctl stop policy-manager`

Answer: C

8. Which of the following does NOT describe Dragon Host Sensors Multi-Detection methods?

- A. Monitors output to a hosts system and audit logs
- B. Monitors a hosts files via MD5 integrity-checking
- C. Monitors a hosts specified network interface promiscuously for anomalous activity
- D. Monitors a hosts specific file attributes for changes to owner, group, permissions and file size
- E. Monitors a Windows hosts Registry for attributes that should not be accessed and/or modified

Answer: C

9. Which of the following best describes the relationship between policies and signatures on a Dragon Host Sensor?

- A. Policies can contain O/S-specific signatures
- B. Signatures can contain O/S-specific policies
- C. Policies and signatures are combined in a single library
- D. Policies and signatures are unrelated

Answer: A

10. What is the recommended method to start all installed Dragon components in Enterprise mode?

- A. `./dragon enterprise`
- B. `./driders enterprise`
- C. `./dragonctl start`
- D. `./dragonctl enterprise`

Answer: C

11. What is one benefit of Dragon Network Sensors dual network interface capability as deployed on a non-Dragon Appliance system?

- A. Secure management and reporting on one interface; Network Sensor invisible on other interface
- B. Allows for collection of event data from both interfaces simultaneously
- C. Allows for protocol detection from one interface, and anomaly detection from the other interface
- D. This functionality is ONLY available on Dragon Appliances

Answer: A

12. Which of the following is NOT a valid detection method used by Dragon Network Sensor?

- A. Signature detection
- B. Protocol detection
- C. Policy detection
- D. Anomaly detection

Answer: C

13. Why might an IDS administrator configure Dragon Enterprise Management Server to INITIATE outbound connections to remote Network/Host Sensors?

- A. To increase performance when traversing a corporate DMZ
- B. To provide the additional security that is inherent in the Server-initiated communication

C. Dragon only allows server-initiated (outbound) connections

D. To integrate Dragon into MSSP or other environments where firewalls prohibit inbound connections from Network/Host Sensors

Answer: D

14. Which of the following is required in order for the Dragon installation script (install.pl) to be completed?

A. Dragon license key

B. Pre-configured user and group named dragon

C. Active link to the internet

Answer: B

15. What two modes are available when installing a Dragon Host Sensor?

A. Standalone and Enterprise

B. Local and Remote

C. Active and Standby

Answer: A

16. How many Dragon Policy Managers can simultaneously manage a single Dragon Network/Host Sensor?

A. 1

B. 2

C. 10

D. Unlimited

Answer: A

17. Which component of Dragon is most responsible for enabling hierarchical deployments?

A. Dragon Network Sensor

B. Dragon Security Information Manager

C. Dragon Event Flow Processor

D. Dragon Hierarchy Agent

Answer: C

18. What might be one benefit of configuring a Dragon Host Sensor Server?

A. To provide IKE-level security for Host Sensors deployed in a corporate DMZ

B. To centrally collect NIDS-event data from Network Sensors

C. To collect HIDS-event data from systems on which it is not possible or practical to deploy a Dragon Host Sensor

Answer: C

19. Which of the following is NOT a function of Dragon Forensics Console?

A. Allows for central configuration of Active Response mechanisms to deter network attacks

B. Centrally analyzes activity as it is occurring or has occurred over time

C. Correlates events together across Network Sensor, Host Sensor, and any other infrastructure system (e.g., firewall, router) for which messages have been received (via Host Sensor log forwarding)

D. Provides the tools for performing a forensics level analysis and reconstructing an attacker's session

Answer: A

20. Which best describes a SYN Flood attack?

A. Attacker redirects unusually large number of SYN/ACK packets

B. Attacker sends relatively large number of altered SYN packets

C. Attacker floods a host with a relatively large number of unaltered SYN packets

D. Attacker floods a host with an unusually large number of legitimate ACK packets

Answer: B

[More 2B0-018 Information](#)

### Related 2B0-018 Exams

[2B0-012](#) *ES Switching Edition 4.0*

[2B0-011](#) *ES Router Configuration*

[2B0-100](#) *Enterasys Systems Engineer (ESE) Recertification*

[2B0-021](#) *ES XSR Configuration*

[2B0-015](#) *ES Wireless*

[2B0-019](#) *ES Policy Enabled Networking*

[2B0-102](#) *Enterasys Security Systems Engineer-Defense*

[2B0-024](#) *ES Secure Networks*

[2B0-104](#) *Enterasys Certified Internetworking Engineer(ECIE)*

[2B0-101](#) *Enterasys Security Systems Engineer (ESSE) Recertification*

[2B0-020](#) *ES NetSight Atlas*

[2B0-022](#) *ES XSR Security*

[2B0-103](#) *Enterasys Security Systems Engineer-NAC*

[2B0-018](#) *ES Dragon IDS*

[2B0-023](#) *ES Advanced Dragon IDS*

### Other Enterasys Networks Exams

[2B0-101](#)

[2B0-102](#)

[2B0-021](#)

[2B0-022](#)

[2B0-012](#)

[2B0-018](#)

[2B0-103](#)

[2B0-024](#)

[2B0-100](#)

[2B0-023](#)

[2B0-011](#)

[2B0-104](#)

[2B0-020](#)

[2B0-019](#)

[2B0-015](#)