



600-199^{Q&As}

Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/600-199.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

When an IDS generates an alert for a correctly detected network attack, what is this event called?

- A. false positive
- B. true negative
- C. true positive
- D. false negative

Correct Answer: C

QUESTION 2

For TCP and UDP, what is the correct range of well-known port numbers?

- A. 0 - 1023
- B. 1 - 1024
- C. 1 - 65535
- D. 0 - 65535
- E. 024 - 65535

Correct Answer: A

QUESTION 3

When is it recommended to establish a traffic profile baseline for your network?

- A. outside of normal production hours
- B. during a DDoS attack
- C. during normal production hours
- D. during monthly file server backup

Correct Answer: C

QUESTION 4

Which three statements are true about the IP fragment offset? (Choose three.)

- A. A fragment offset of 0 indicates that it is the first in a series of fragments.



- B. A fragment offset helps determine the position of the fragment within the reassembled datagram.
- C. A fragment offset number refers to the number of fragments.
- D. A fragment offset is measured in 8-byte units.
- E. A fragment offset is measured in 16-byte units.

Correct Answer: ABD

QUESTION 5

Which event is likely to be a false positive?

- A. Internet Relay Chat signature with an alert context buffer containing #IPS_ROCS Yay
- B. a signature addressing an ActiveX vulnerability alert on a Microsoft developer network documentation page
- C. an alert for a long HTTP request with an alert context buffer containing a large HTTP GET request
- D. BitTorrent activity detected on ephemeral ports

Correct Answer: B

[600-199 VCE Dumps](#)

[600-199 Practice Test](#)

[600-199 Exam Questions](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4itsure.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © pass4itsure, All Rights Reserved.