



# 500-290<sup>Q&As</sup>

IPS Express Security for Engineers

## Pass Cisco 500-290 Exam with 100% Guarantee

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

<https://www.lead4pass.com/500-290.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

Context Explorer can be accessed by a subset of user roles. Which predefined user role is valid for FireSIGHT event access?

- A. Administrator
- B. Intrusion Administrator
- C. Maintenance User
- D. Database Administrator

Correct Answer: A

---

### QUESTION 2

Which statement describes the meaning of a red health status icon?

- A. A critical threshold has been exceeded.
- B. At least one health module has failed.
- C. A health policy has been disabled on a monitored device.
- D. A warning threshold has been exceeded.

Correct Answer: A

---

### QUESTION 3

A one-to-many type of scan, in which an attacker uses a single host to scan a single port on multiple target hosts, indicates which port scan type?

- A. port scan
- B. portsweep
- C. decoy port scan
- D. ACK scan

Correct Answer: B

---

### QUESTION 4

When configuring FireSIGHT detection, an administrator would create a network discovery policy and set the action to "discover". Which option is a possible type of discovery?



- A. host
- B. IPS event
- C. anti-malware
- D. networks

Correct Answer: A

---

#### QUESTION 5

Which option describes Spero file analysis?

- A. a method of analyzing the SHA-256 hash of a file to determine whether a file is malicious or not
- B. a method of analyzing the entire contents of a file to determine whether it is malicious or not
- C. a method of analyzing certain file characteristics, such as metadata and header information, to determine whether a file is malicious or not
- D. a method of analyzing a file by executing it in a sandbox environment and observing its behaviors to determine if it is malicious or not

Correct Answer: C

[Latest 500-290 Dumps](#)

[500-290 Study Guide](#)

[500-290 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.lead4pass.com/allproducts>

## Need Help

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



 <p><b>One Year Free Update</b> 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>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; 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 © lead4pass, All Rights Reserved.