



500-275^{Q&As}

Securing Cisco Networks with Sourcefire FireAMP Endpoints
(SSFAMP)

Pass Cisco 500-275 Exam with 100% Guarantee

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

<https://www.lead4pass.com/500-275.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

What is the default command-line switch configuration, if you run a connector installation with no parameters?

- A. /desktopicon 0 /startmenu 1 /contextmenu 1 /skipdfc 0 /skiptetra 0
- B. /desktopicon 1 /startmenu 0 /contextmenu 0 /skipdfc 0 /skiptetra 0
- C. /desktopicon 0 /startmenu 0 /contextmenu 0 /skipdfc 1 /skiptetra 1
- D. /desktopicon 1 /startmenu 0 /contextmenu 0 /skipdfc 0 /skiptetra 1

Correct Answer: A

QUESTION 2

When discussing the FireAMP product, which term does the acronym DFC represent?

- A. It means Detected Forensic Cause.
- B. It means Duplicate File Contents.
- C. It means Device Flow Correlation.
- D. It is not an acronym that is associated with the FireAMP product.

Correct Answer: C

QUESTION 3

Which option is a detection technology that is used by FireAMP?

- A. fuzzy matching
- B. Norton AntiVirus
- C. network scans
- D. Exterminator

Correct Answer: A

QUESTION 4

When you are viewing information about a computer, what is displayed?

- A. the type of antivirus software that is installed
- B. the internal IP address



- C. when the operating system was installed
- D. the console settings

Correct Answer: B

QUESTION 5

The FireAMP connector monitors the system for which type of activity?

- A. Vulnerabilities
- B. Enforcement of usage policies
- C. File operations
- D. Authentication activity

Correct Answer: C

QUESTION 6

The Accounts menu contains items that are related to FireAMP console accounts. Which menu allows you to set the default group policy?

- A. Audit Log
- B. Users
- C. Applications
- D. Business

Correct Answer: D

QUESTION 7

How does application blocking enhance security?

- A. It identifies and logs usage.
- B. It tracks application abuse.
- C. It deletes identified applications.
- D. It blocks vulnerable applications from running, until they are patched.

Correct Answer: D



QUESTION 8

Which set of actions would you take to create a simple custom detection?

- A. Add a SHA-256 value; upload a file to calculate a SHA-256 value; upload a text file that contains SHA- 256 values.
- B. Upload a packet capture; use a Snort rule; use a ClamAV rule.
- C. Manually input the PE header data, the MD-5 hash, and a list of MD-5 hashes.
- D. Input the file and file name.

Correct Answer: A

QUESTION 9

The Update Window allows you to perform which action?

- A. identify which hosts need to be updated
- B. email the user to download a new client
- C. specify a timeframe when an upgrade can be started and stopped
- D. update your cloud instance

Correct Answer: C

QUESTION 10

What is the first system that is infected with a particular malware called?

- A. Patient Zero
- B. Source
- C. Infector
- D. Carrier

Correct Answer: A

QUESTION 11

Which question should be in your predeployment checklist?

- A. How often are backup jobs run?
- B. Are any Linux servers being deployed?
- C. Who are the users of the hosts on which you will deploy?



D. Which applications are installed on the hosts on which you will deploy?

Correct Answer: D

QUESTION 12

Which feature allows retrospective detection?

- A. Total Recall
- B. Cloud Recall
- C. Recall Alert
- D. Recall Analysis

Correct Answer: B

QUESTION 13

Which disposition can be returned in response to a malware cloud lookup?

- A. Dirty
- B. Virus
- C. Malware
- D. Infected

Correct Answer: C

QUESTION 14

Which information does the File Trajectory feature show?

- A. the time that the scan was run
- B. the name of the file
- C. the hosts on which the file was seen and points in time where events occurred
- D. the protocol

Correct Answer: C

QUESTION 15

Which of these can you use for two-step authentication?



- A. the Apple Authenticator app
- B. the Google Authenticator app
- C. a SecurID token
- D. any RFC 1918 compatible application

Correct Answer: B

[500-275 PDF Dumps](#)

[500-275 VCE Dumps](#)

[500-275 Study Guide](#)



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

Try our product !

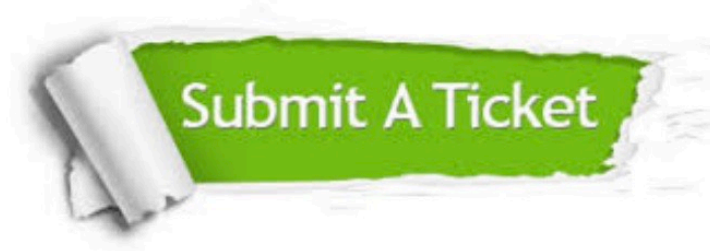
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [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>One Year Free Update 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>Money Back Guarantee 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>Security & Privacy 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 © lead4pass, All Rights Reserved.