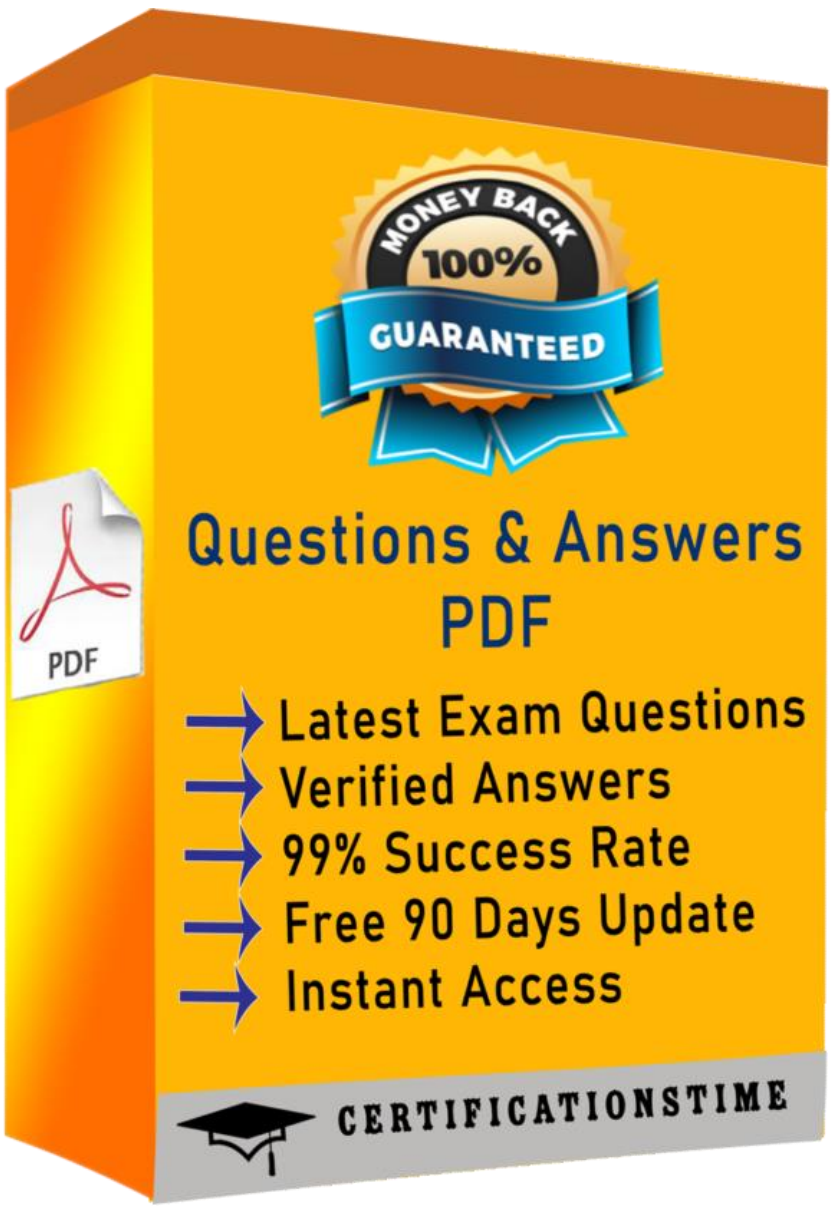
Cisco

Exam Questions 500-275

SSFAMP Securing Cisco Networks with Sourcefire FireAMP Endpoints

https://certificationstime.com/



Question 1

Which option is one of the three methods of updating the IP addresses in Sourcefire Security Intelligence?
A. subscribe to a URL intelligence feed
B. subscribe to a VRT
C. upload a list that you create
D. automatically upload lists from a network share
Answer: C

Question 2

Which statement is true in regard to the Sourcefire Security Intelligence lists?
A. The global blacklist universally allows all traffic through the managed device.
B. The global whitelist cannot be edited.
C. IP addresses can be added to the global blacklist by clicking on interactive graphs in Context Explorer.
D. The Security Intelligence lists cannot be updated.
Answer: C

Question 3

When building a platform for a Snort installation, which set of components is a major security concern?
A. IP address, mask, and gateway settings
B. host naming conventions
C. URL feed vendors
D. default accounts and settings
Answer: D

Question 4

In the IP addressing scheme of your organization, each subnet consists of 4096 hosts, and the beginning of the addressing scheme is 172.16.0.0. Your remote office is allocated the range of addresses from the first subnet. What are the CIDR notation, network address, broadcast address, and valid IP address in your assigned range?
A. 172.16.0.0/24, 172.16.0.0, 172.16.8.255, 172.16.0.51
B. 172.16.0.0/20, 172.16.0.0, 172.16.15.255, 172.16.8.252
C. 172.16.0.0/16, 172.16.0.0, 172.16.32.255, 172.16.22.4
D. 172.16.0.0/12, 172.16.0.0, 172.16.64.255, 172.16.52.112
Answer: B

Question 5

Which statement about implementing DAQ is true?
A. It is a shell script that works on any Linux platform.
B. It must be compiled separately.
C. You must obtain it from Sourceforge.
D. It is not open source.
Answer: B

Question 6

Which version of libpcap does DAQ require?
A. 0.9.8 or later
B. 1.0.0 or later
C. any version
D. none
Answer: B

Question 7

If Snort is installed and the sensor, database, and web server all reside on the same machine, to which ports should remote access of the sensor be restricted?
A. 22 and 443
B. 80 and 443
C. 443 and 3306
D. 23 and 80
Answer: A

Question 8

To execute a command in Linux while in the directory where it is located, and be sure you are only running that particular copy, what would you use in front of the executable name?
A. ./
B. ../
C. ..\
D. .\
Answer: A