

DUMPSBOSS.

Securing Cisco Networks with Sourcefire FireAMP Endpoints

Cisco 500-275

Version Demo

Total Demo Questions: 10

Total Premium Questions: 50

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, FireAMP Overview and Architecture	9
Topic 2, Outbreak Control Menu Items	5
Topic 3, Endpoint Policies	5
Topic 4, Groups and Development	6
Topic 5, Analysis and Reporting	9
Topic 6, Private Cloud	5
Topic 7, Accounts	3
Topic 8, FireAMP Connector	3
Topic 9, Console Interface	5
Total	50

QUESTION NO: 1

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

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

ANSWER: C

QUESTION NO: 2

Which statement describes an advantage of cloud-based detection?

- A. Limited customization allows for faster detection.
- B. Fewer resources are required on the endpoint.
- C. Sandboxing reduces the overall management overhead of the system.
- D. High-speed analytical engines on the endpoint limit the amount of work the cloud must perform.

ANSWER: B

QUESTION NO: 3

For connector-to-FireAMP Private Cloud communication, which port number is used for lower-overhead communication?

- A. 22
- B. 80
- C. 443
- D. 32137

ANSWER: D

QUESTION NO: 4

What is a valid data source for DFC Windows connector policy configuration?

- A. SANS
- B. NIST
- C. Emerging Threats
- D. Custom and Sourcefire

ANSWER: D

QUESTION NO: 5

How can customers feed new intelligence such as files and hashes to FireAMP?

- A. by uploading it to the FTP server
- B. from the connector
- C. through the management console
- D. by sending it via email

ANSWER: C

QUESTION NO: 6

What is the default clean disposition cache setting?

- A. 3600
- B. 604800
- C. 10080
- D. 1 hour

ANSWER: B

QUESTION NO: 7

Which hosts merit special consideration for crafting a policy?

- A. end-user hosts

- B. domain controllers
- C. Linux servers
- D. none, because all hosts should get equal consideration

ANSWER: B

QUESTION NO: 8

Which pair represents equivalent processes whose names differ, depending on the connector version that you are running?

- A. immuneset_protect and iptray
- B. agent.exe and sfc.exe
- C. TETRA and SPERO
- D. ETHOS and SPERO

ANSWER: B

QUESTION NO: 9

Incident responders use which policy mode for outbreak control?

- A. Audit
- B. Protect
- C. Triage
- D. Emergency

ANSWER: C

QUESTION NO: 10

If a file's SHA-256 hash is sent to the cloud, but the cloud has never seen the hash before, which disposition is returned?

- A. Clean
- B. Neutral
- C. Malware

D. Unavailable

ANSWER: B