DUMPSBOSS.

Securing Cisco Networks with Sourcefire FireAMP Endpoints

Cisco 500-275

Version Demo

Total Demo Questions: 7

Total Premium Questions: 71

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Components	17
Topic 2, Deployment	13
Topic 3, Policies	18
Topic 4, Analysis and Troubleshooting	23
Total	71

QUESTION NO: 1

Which FireAMP capability allows a file that was initially classified as clean to be identified later as malicious?

A. Retrospective security

B. Application blocking

C. Connector update window

D. Two-step authentication

ANSWER: A

Explanation:

Retrospective security is correct. FireAMP continuously monitors files after their initial disposition. If Cisco threat intelligence later changes a file disposition to Malware, FireAMP can identify the endpoints on which the file was previously observed and generate the appropriate detection and response activity.

This capability is important because a file reputation can change after additional global telemetry or analysis becomes available. See Cisco Secure Endpoint for current product information.

QUESTION NO: 2

Which action is appropriate after a quarantined file is confirmed to be a false positive?

A. Restore the file from quarantine.

B. Delete the endpoint group.

C. Disable all cloud lookups.

D. Uninstall the connector from every computer.

ANSWER: A

Explanation:

Restore the file from quarantine is correct. After investigation confirms that a detected file is legitimate, an authorized administrator can restore it so that it is returned to its original endpoint location. The administrator should also evaluate whether a carefully scoped exclusion or custom whitelist is needed to prevent repeated false-positive detections.

Restoration should be performed only after the file's legitimacy has been verified. See the Cisco Secure Endpoint user-guide library for current operational guidance.

QUESTION NO: 3

From the Deployment screen, you can deploy agents via which mechanism?

A. push to client

B. .zip install file

C. user download from Sourcefire website or email

D. precompiled RPM package

ANSWER: C

Explanation:

The correct mechanism is **user download from Sourcefire website or email**. In the FireAMP for Endpoints (now Cisco Secure Endpoint) management console, the Deployment area is used to generate and obtain a connector installer for the selected operating system and policy. An administrator can download the installer directly and make it available to users, or distribute the download information through email so that users can retrieve and install the connector. This workflow supports deployments in which endpoint users perform the installation themselves while the connector registers to the organization's cloud console and receives the appropriate policy.

The deployment process is centered on obtaining the platform-specific connector package and providing it to the endpoint, rather than the console directly initiating a remote installation. The installer associated with the deployment configuration ensures that the installed connector is linked to the correct Secure Endpoint tenant and policy context. Cisco's Secure Endpoint documentation describes downloading connector installers from the console and using those installers for endpoint deployment. See the Cisco Secure Endpoint User Guide and Cisco's Secure Endpoint product documentation page.

QUESTION NO: 4

Which type of exclusion is most appropriate when an approved application creates high-volume temporary files in one known directory?

A. A path exclusion for the known directory

B. A whitelist for every executable on the endpoint

C. A policy that disables all file protection

D. A File Trajectory exclusion

ANSWER: A

Explanation:

A narrowly scoped path exclusion for the known directory is the most appropriate choice. It reduces unnecessary scanning of the application's temporary files while avoiding a broad exception that could create unnecessary exposure elsewhere on the endpoint. Exclusions should be limited to documented business requirements and reviewed regularly. Cisco Secure Endpoint policy and connector guidance is available from the Cisco Secure Endpoint User Guide library.

QUESTION NO: 5

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

ANSWER: B

Explanation:

The Google Authenticator app can be used for two-step authentication because it generates time-based, one-time passcodes that are entered in addition to the user's normal username and password. In Cisco Secure Endpoint (formerly AMP for Endpoints), two-step authentication is configured by associating an authenticator application with the user account through a QR-code enrollment process. After enrollment, the application produces a short-lived verification code that provides the additional authentication factor at sign-in.

Google Authenticator implements the standard time-based one-time password approach, allowing the authentication service and the enrolled mobile application to calculate matching codes from a shared secret and the current time. This provides a

practical second factor without requiring a separate hardware device. Cisco's Secure Endpoint documentation describes two-step authentication as an account-access protection feature, while Google documents how its Authenticator application creates verification codes for two-step verification. See the Cisco Secure Endpoint support documentation and Google Authenticator help.

QUESTION NO: 6

Which option represents a configuration step on first use?

A. Verify, Contain, and Protect

B. User Account Setup

C. System Defaults Configuration

D. Event Filtering

ANSWER: B

Explanation:

User Account Setup is a first-use configuration step because Secure Endpoint (formerly AMP for Endpoints) requires the initial administrator to establish and manage console user access before routine operational administration can be performed. User setup defines who may sign in to the cloud console and assigns the permissions needed to manage endpoint groups, policies, connectors, events, and investigations. This is foundational configuration: the organization must have appropriately authorized administrative identities so that administration is accountable, access is controlled according to job function, and subsequent configuration can be performed securely. In practice, administrators create or invite users and apply suitable roles based on the responsibilities delegated to them. This supports least-privilege access and enables teams such as security operations and endpoint administration to use the console without sharing credentials. Cisco identifies Secure Endpoint as the current product family for AMP for Endpoints and provides product documentation and support resources through its official Secure Endpoint portal. See the Cisco Secure Endpoint support page and the Cisco Secure Endpoint documentation portal for current product resources, including console administration and access-management information.

QUESTION NO: 7

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

ANSWER: B

Explanation:

When viewing a computer's details in the Cisco Secure Endpoint (formerly AMP for Endpoints) console, the internal IP address is displayed as part of the endpoint information collected by the Secure Endpoint connector. This information helps an administrator identify the host on its local network, investigate endpoint activity, and correlate events shown in the console with other network-security telemetry. A computer record is designed to provide useful device and connector details, including network-related information, so the internal IP address is an appropriate attribute to expect in the computer-information view.

Cisco Secure Endpoint provides endpoint visibility and management through its cloud console, where administrators can review individual computer records and investigate the device context associated with security events. The product

documentation and support resources for Secure Endpoint are available through Cisco Secure Endpoint and Cisco Secure Endpoint User Guides.