250-428^{Q&As}

250-428^{Q&As}

Administration of Symantec Endpoint Protection 14

Pass Symantec 250-428 Exam with 100% Guarantee

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

https://www.pass2lead.com/250-428.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Symantec Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

Which ports on the company firewall must an administrator open to avoid problems when connecting to Symantec Public LiveUpdate servers?

A. 25, 80, and 2967

B. 2967, 8014, and 8443

C. 21, 443, and 2967

D. 21, 80, and 443

Correct Answer: D

QUESTION 2

Which action does the Shared Insight Cache (SIC) server take when the whitelist reaches maximum capacity?

A. The SIC server allocates additional memory for the whitelist as needed.

B. The SIC server will start writing the cache to disk.

C. The SIC server will remove the least recently used items based on the prune size.

D. The SIC server will remove items with the fewest number of votes.

Correct Answer: C

QUESTION 3

A Symantec Endpoint Protection (SEP) administrator creates a firewall policy to block FTP traffic and assigns the policy to all of the SEP clients. The network monitoring team informs the administrator that a client system is making an FTP connection to a server. While investigating the problem from the SEP client GUI, the administrator notices that there are zero entries pertaining to FTP traffic in the SEP Traffic log or Packet log. While viewing the Network Activity dialog, there is zero inbound/outbound traffic for the FTP process.

What is the most likely reason?

A. The block rule is below the blue line.

B. The server has an IPS exception for that traffic.

C. Peer-to-peer authentication is allowing the traffic.

D. The server is in the IPS policy excluded hosts list.

Correct Answer: D

QUESTION 4

The Security Status on the console home page is failing to alert a Symantec Endpoint Protection (SEP) administrator when virus definitions are out of date.

How should the SEP administrator enable the Security Status alert?

A. Lower the Security Status thresholds

B. Raise the Security Status thresholds

C. Change the Notifications setting to "Show all notifications"

D. Change the Action Summary display to "By number of computers"

Correct Answer: A

References: https://support.symantec.com/en_US/article.HOWTO81151.html

QUESTION 5

A company deploys Symantec Endpoint Protection client to its sales staff who travel across the country. Which deployment method should the company use to notify its sales staff to install the client?

A. Push mode

B. Client Deployment Wizard

C. Pull mode

D. Unmanaged Detector

Correct Answer: B

References: https://support.symantec.com/en_US/article.HOWTO80787.html#v16194660