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.geekcert.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

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 3

An organization is troubleshooting a SONAR false positive and has created an exclusion for the in-house application generating the detection. How can the organization use Process Explorer to verify that the exclusion works?

A. Use Process Explorer to see if secars.dll is still there. If secars.dll is still present in the application as an injected process, ensure the updated policy is applied to the group

B. Use Process Explorer to see if UMEngx86.dll is still there. If UMEngx86.dll is still present in the application as an injected process, ensure the updated policy is applied to the group

C. Use Process Explorer to see if IPSFFPI.dll is still there. If IPSFFPI.dll is still present in the application as an injected process, ensure the updated policy is applied to the group

D. Use Process Explorer to see if sysfer.dll is still there. If sysfer.dll is still present in the application as an injected process, ensure the updated policy is applied to the group

Correct Answer: D

QUESTION 4

Solusell recently deployed SEP 14 in their environment and created the following groups for their computers: Desktops Laptops Servers

What type of group structure does Solusell use?

A. Role

B. Combination

C. Folder

D. Geography

Correct Answer: C

Reference: https://support.symantec.com/us/en/article.tech134409.html

QUESTION 5

What two core technologies does Symantec Endpoint Protection firewall utilize? (Choose two.)

A. Circuit-level gateway

B. Packet filtering

C. Stateful

D. Application-level gateway

E. Deep packet inspection

Correct Answer: BC

Reference: https://support.symantec.com/us/en/article.HOWTO80961.html