350-701 Q&As

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

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

https://www.passapply.com/350-701.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

For which two conditions can an endpoint be checked using ISE posture assessment? (Choose two)

A. Windows service

B. computer identity

C. user identity

D. Windows firewall

E. default browser

Correct Answer: AD

QUESTION 2

What are two ways a network administrator transparently identifies users using Active Directory on the Cisco WSA? (Choose two.)

A. The eDirectory client must be installed on each client workstation.

B. Create NTLM or Kerberos authentication realm and enable transparent user identification

C. Deploy a separate Active Directory agent such as Cisco Context Directory Agent.

D. Create an LDAP authentication realm and disable transparent user identification.

E. Deploy a separate eDirectory server: the client IP address is recorded in this server

Correct Answer: AB

Details:

https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-0/user_guide/b_WSA_UserGuide/b_WSA_UserGuide_chapter_01001.html#:~:text=Transparently%20identify%20users%20with%20authentication,User%20Identification%20with%

20 LDAP.

QUESTION 3

What are two list types within AMP for Endpoints Outbreak Control? (Choose two)

A. blocked ports

B. simple custom detections

C. command and control

D. allowed applications

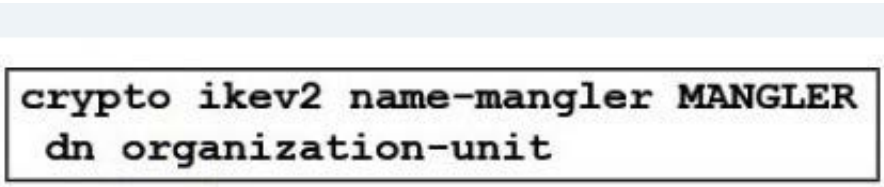
E. URL

Correct Answer: BD

Advanced Malware Protection (AMP) for Endpoints offers a variety of lists, referred to as Outbreak Control, that allow you to customize it to your needs. The main lists are: Simple Custom Detections, Blocked Applications, Allowed Applications, Advanced Custom Detections, and IP Blocked and Allowed Lists.A Simple Custom Detection list is similar to a blocked list. These are files that you want to detect andquarantine.Allowed applications lists are for files you never want to convict. Some examples are a custom application that is detected by a generic engine or a standard image that you use throughout the company Reference:
https://docs.amp.cisco.com/AMP%20for%20Endpoints%20User%20Guide.pdf

QUESTION 4

Refer to the exhibit.



An engineer is implementing a certificate based VPN. What is the result of the existing configuration?

A. The OU of the IKEv2 peer certificate is used as the identity when matching an IKEv2 authorization policy.

B. Only an IKEv2 peer that has an OU certificate attribute set to MANGLER establishes an IKEv2 SA successfully

C. The OU of the IKEv2 peer certificate is encrypted when the OU is set to MANGLER

D. The OU of the IKEv2 peer certificate is set to MANGLER

Correct Answer: A

The "match identity certificate" command in the IKEv2 authorization policy is used to specify that the OU (Organizational Unit) attribute of the IKEv2 peer certificate should be used as the identity when matching the policy. The OU attribute is set to "MANGLER" in this case.

So, when an IKEv2 peer with a certificate that has an OU attribute of "MANGLER" attempts to establish an IKEv2 SA, the router will use the OU attribute as the identity when matching the authorization policy. If the policy is a match, the SA will be established successfully.

QUESTION 5

Which solution is more secure than the traditional use of a username and password and encompasses at least two of the methods of authentication?

A. RADIUS/LDAP authentication

B. single-sign on

C. Kerberos security solution

D. multifactor authentication

Correct Answer: D