

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

<https://www.2passeasy.com/dumps/350-701/>



NEW QUESTION 1

Which feature requires a network discovery policy on the Cisco Firepower Next Generation Intrusion Prevention System?

- A. security intelligence
- B. impact flags
- C. health monitoring
- D. URL filtering

Answer: A

NEW QUESTION 2

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

- A. correlation
- B. intrusion
- C. access control
- D. network discovery

Answer: D

NEW QUESTION 3

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

- A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
- B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
- C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
- D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
- E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Answer: BC

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.html

NEW QUESTION 4

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

- A. Application Control
- B. Security Category Blocking
- C. Content Category Blocking
- D. File Analysis

Answer: B

Explanation:

Reference: <https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories>

NEW QUESTION 5

Which algorithm provides encryption and authentication for data plane communication?

- A. AES-GCM
- B. SHA-96
- C. AES-256
- D. SHA-384

Answer: A

NEW QUESTION 6

DRAG DROP

Drag and drop the capabilities from the left onto the correct technologies on the right.

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	superior threat prevention and mitigation for known and unknown threats
superior threat prevention and mitigation for known and unknown threats	detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	combined integrated solution of strong defense and web protection, visibility, and controlling solutions

NEW QUESTION 7

How does Cisco Umbrella archive logs to an enterprise- owned storage?

- A. by using the Application Programming Interface to fetch the logs
- B. by sending logs via syslog to an on-premises or cloud-based syslog server
- C. by the system administrator downloading the logs from the Cisco Umbrella web portal
- D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

Explanation:

Reference: <https://docs.umbrella.com/deployment-umbrella/docs/log-management>

NEW QUESTION 8

Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. Firepower
- C. FireSIGHT
- D. ASA

Answer: A

NEW QUESTION 9

Which benefit does endpoint security provide the overall security posture of an organization?

- A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
- B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
- C. It allows the organization to detect and respond to threats at the edge of the network.

D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Answer: D

NEW QUESTION 10

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

- A. computer identity
- B. Windows service
- C. user identity
- D. Windows firewall
- E. default browser

Answer: BC

NEW QUESTION 10

Where are individual sites specified to be blacklisted in Cisco Umbrella?

- A. application settings
- B. content categories
- C. security settings
- D. destination lists

Answer: D

NEW QUESTION 12

Which ID store requires that a shadow user be created on Cisco ISE for the admin login to work?

- A. RSA SecureID
- B. Internal Database
- C. Active Directory
- D. LDAP

Answer: C

NEW QUESTION 13

An engineer needs a solution for TACACS+ authentication and authorization for device administration. The engineer also wants to enhance wired and wireless network security by requiring users and endpoints to use 802.1X, MAB, or WebAuth. Which product meets all of these requirements?

- A. Cisco Prime Infrastructure
- B. Cisco Identity Services Engine
- C. Cisco Stealthwatch
- D. Cisco AMP for Endpoints

Answer: B

NEW QUESTION 18

Which API is used for Content Security?

- A. NX-OS API
- B. IOS XR API
- C. OpenVuln API
- D. AsyncOS API

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12/test_chapter_01.html

NEW QUESTION 21

Under which two circumstances is a CoA issued? (Choose two.)

- A. A new authentication rule was added to the policy on the Policy Service node.
- B. An endpoint is deleted on the Identity Service Engine server.
- C. A new Identity Source Sequence is created and referenced in the authentication policy.
- D. An endpoint is profiled for the first time.
- E. A new Identity Service Engine server is added to the deployment with the Administration persona.

Answer: BD

Explanation:

Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

NEW QUESTION 26

An engineer used a posture check on a Microsoft Windows endpoint and discovered that the MS17-010 patch was not installed, which left the endpoint vulnerable

to WannaCry ransomware. Which two solutions mitigate the risk of this ransomware infection? (Choose two.)

- A. Configure a posture policy in Cisco Identity Services Engine to install the MS17-010 patch before allowing access on the network.
- B. Set up a profiling policy in Cisco Identity Service Engine to check and endpoint patch level before allowing access on the network.
- C. Configure a posture policy in Cisco Identity Services Engine to check that an endpoint patch level is met before allowing access on the network.
- D. Configure endpoint firewall policies to stop the exploit traffic from being allowed to run and replicate throughout the network.
- E. Set up a well-defined endpoint patching strategy to ensure that endpoints have critical vulnerabilities patched in a timely fashion.

Answer: AC

NEW QUESTION 31

Which ASA deployment mode can provide separation of management on a shared appliance?

- A. DMZ multiple zone mode
- B. transparent firewall mode
- C. multiple context mode
- D. routed mode

Answer: C

NEW QUESTION 32

What provides visibility and awareness into what is currently occurring on the network?

- A. CMX
- B. WMI
- C. Prime Infrastructure
- D. Telemetry

Answer: C

NEW QUESTION 37

Which attack is commonly associated with C and C++ programming languages?

- A. cross-site scripting
- B. water holing
- C. DDoS
- D. buffer overflow

Answer: D

Explanation:

Reference: https://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION 40

Which feature within Cisco Umbrella allows for the ability to inspect secure HTTP traffic?

- A. File Analysis
- B. SafeSearch
- C. SSL Decryption
- D. Destination Lists

Answer: C

NEW QUESTION 43

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 350-701 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 350-701 Product From:

<https://www.2passeasy.com/dumps/350-701/>

Money Back Guarantee

350-701 Practice Exam Features:

- * 350-701 Questions and Answers Updated Frequently
- * 350-701 Practice Questions Verified by Expert Senior Certified Staff
- * 350-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 350-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year