

Cisco

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



NEW QUESTION 1

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 2

Which technology reduces data loss by identifying sensitive information stored in public computing environments?

- A. Cisco SDA
- B. Cisco Firepower
- C. Cisco HyperFlex
- D. Cisco Cloudlock

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/dam/en/us/products/collateral/security/cloudlock/cisco-cloudlock-cloud-data-security-datasheet.pdf>

NEW QUESTION 3

Refer to the exhibit.

```
snmp-server group SNMP v3 auth access 15
```

What does the number 15 represent in this configuration?

- A. privilege level for an authorized user to this router
- B. access list that identifies the SNMP devices that can access the router
- C. interval in seconds between SNMPv3 authentication attempts
- D. number of possible failed attempts until the SNMPv3 user is locked out

Answer: B

NEW QUESTION 4

Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

- A. Nexus
- B. Stealthwatch
- C. Firepower
- D. Tetration

Answer: D

Explanation:

Reference: <https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/index.html#~products>

NEW QUESTION 5

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 6

Which two descriptions of AES encryption are true? (Choose two.)

- A. AES is less secure than 3DES.
- B. AES is more secure than 3DES.
- C. AES can use a 168-bit key for encryption.
- D. AES can use a 256-bit key for encryption.
- E. AES encrypts and decrypts a key three times in sequence.

Answer: BD

Explanation:

Reference: https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html

NEW QUESTION 7

An engineer configured a new network identity in Cisco Umbrella but must verify that traffic is being routed through the Cisco Umbrella network. Which action tests the routing?

- A. Ensure that the client computers are pointing to the on-premises DNS servers.
- B. Enable the Intelligent Proxy to validate that traffic is being routed correctly.
- C. Add the public IP address that the client computers are behind to a Core Identity.
- D. Browse to <http://welcome.umbrella.com/> to validate that the new identity is working.

Answer: B

NEW QUESTION 8

Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

- A. NGFW
- B. AMP
- C. WSA
- D. ESA

Answer: B

NEW QUESTION 9

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 10

Which two activities can be done using Cisco DNA Center? (Choose two.)

- A. DHCP
- B. design
- C. accounting
- D. DNS
- E. provision

Answer: BE

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_1_chapter_00.pdf

NEW QUESTION 10

How is ICMP used as an exfiltration technique?

- A. by flooding the destination host with unreachable packets
- B. by sending large numbers of ICMP packets with a targeted host's source IP address using an IP broadcast address
- C. by encrypting the payload in an ICMP packet to carry out command and control tasks on a compromised host
- D. by overwhelming a targeted host with ICMP echo-request packets

Answer: C

NEW QUESTION 11

What is the difference between deceptive phishing and spear phishing?

- A. Deceptive phishing is an attack aimed at a specific user in the organization who holds a C-level role.
- B. A spear phishing campaign is aimed at a specific person versus a group of people.
- C. Spear phishing is when the attack is aimed at the C-level executives of an organization.
- D. Deceptive phishing hijacks and manipulates the DNS server of the victim and redirects the user to a false webpage.

Answer: B

NEW QUESTION 14

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 18

Which feature is supported when deploying Cisco ASAv within AWS public cloud?

- A. multiple context mode
- B. user deployment of Layer 3 networks
- C. IPv6
- D. clustering

Answer: B

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav-aws.html>

NEW QUESTION 22

Which technology must be used to implement secure VPN connectivity among company branches over a private IP cloud with any-to-any scalable connectivity?

- A. DMVPN
- B. FlexVPN
- C. IPsec DVTI
- D. GET VPN

Answer: D

NEW QUESTION 23

What is the primary role of the Cisco Email Security Appliance?

- A. Mail Submission Agent
- B. Mail Transfer Agent
- C. Mail Delivery Agent
- D. Mail User Agent

Answer: B

NEW QUESTION 26

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

- A. Sophos engine
- B. white list
- C. RAT
- D. outbreak filters
- E. DLP

Answer: AD

NEW QUESTION 30

What is a characteristic of traffic storm control behavior?

- A. Traffic storm control drops all broadcast and multicast traffic if the combined traffic exceeds the level within the interval.
- B. Traffic storm control cannot determine if the packet is unicast or broadcast.
- C. Traffic storm control monitors incoming traffic levels over a 10-second traffic storm control interval.
- D. Traffic storm control uses the Individual/Group bit in the packet source address to determine if the packet is unicast or broadcast.

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html>

NEW QUESTION 32

Which two request of REST API are valid on the Cisco ASA Platform? (Choose two.)

- A. put
- B. options
- C. get
- D. push
- E. connect

Answer: AC

Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html>

NEW QUESTION 37

Which two deployment model configurations are supported for Cisco FTDv in AWS? (Choose two.)

- A. Cisco FTDv configured in routed mode and managed by an FMCv installed in AWS
- B. Cisco FTDv with one management interface and two traffic interfaces configured
- C. Cisco FTDv configured in routed mode and managed by a physical FMC appliance on premises
- D. Cisco FTDv with two management interfaces and one traffic interface configured
- E. Cisco FTDv configured in routed mode and IPv6 configured

Answer: AC

Explanation:

Reference: <https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html>

NEW QUESTION 41

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 46

Which two prevention techniques are used to mitigate SQL injection attacks? (Choose two.)

- A. Check integer, float, or Boolean string parameters to ensure accurate values.
- B. Use prepared statements and parameterized queries.
- C. Secure the connection between the web and the app tier.
- D. Write SQL code instead of using object-relational mapping libraries.
- E. Block SQL code execution in the web application database login.

Answer: AB

Explanation:

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

NEW QUESTION 48

Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

- A. quality of service
- B. time synchronization
- C. network address translations
- D. intrusion policy

Answer: B

NEW QUESTION 52

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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 First Try
- * 350-701 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 350-701 Practice Test Here](#)