

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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



#### NEW QUESTION 1

Refer to the exhibit.

```
aaa new-model

radius-server host 10.0.0.12 key secret12
```

Which statement about the authentication protocol used in the configuration is true?

- A. The authentication request contains only a password
- B. The authentication request contains only a username
- C. The authentication and authorization requests are grouped in a single packet.
- D. There are separate authentication and authorization request packets.

**Answer: C**

#### NEW QUESTION 2

Which two preventive measures are used to control cross-site scripting? (Choose two.)

- A. Enable client-side scripts on a per-domain basis.
- B. Incorporate contextual output encoding/escaping.
- C. Disable cookie inspection in the HTML inspection engine.
- D. Run untrusted HTML input through an HTML sanitization engine.
- E. SameSite cookie attribute should not be used.

**Answer: AB**

#### NEW QUESTION 3

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 4

Which two capabilities does TAXII support? (Choose two.)

- A. exchange
- B. pull messaging
- C. binding
- D. correlation
- E. mitigating

**Answer: BC**

#### NEW QUESTION 5

An administrator wants to ensure that all endpoints are compliant before users are allowed access on the corporate network. The endpoints must have the corporate antivirus application installed and be running the latest build of Windows 10. What must the administrator implement to ensure that all devices are compliant before they are allowed on the network?

- A. Cisco Identity Services Engine and AnyConnect Posture module
- B. Cisco Stealthwatch and Cisco Identity Services Engine integration
- C. Cisco ASA firewall with Dynamic Access Policies configured
- D. Cisco Identity Services Engine with PxGrid services enabled

**Answer: A**

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect46/administration/guide/b\\_AnyConnect\\_Administrator\\_Guide\\_4-6/configure-posture.html](https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect46/administration/guide/b_AnyConnect_Administrator_Guide_4-6/configure-posture.html)

#### NEW QUESTION 6

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

- A. smurf
- B. distributed denial of service
- C. cross-site scripting
- D. rootkit exploit

**Answer: C**

#### NEW QUESTION 7

What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services? (Choose two.)

- A. TACACS+
- B. central web auth
- C. single sign-on
- D. multiple factor auth
- E. local web auth

**Answer:** BE

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin\\_guide/b\\_ise\\_admin\\_guide\\_22/b\\_ise\\_admin\\_guide\\_22\\_chapter\\_01110.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01110.html)

#### NEW QUESTION 8

Which flaw does an attacker leverage when exploiting SQL injection vulnerabilities?

- A. user input validation in a web page or web application
- B. Linux and Windows operating systems
- C. database
- D. web page images

**Answer:** C

#### Explanation:

Reference: [https://tools.cisco.com/security/center/resources/sql\\_injection](https://tools.cisco.com/security/center/resources/sql_injection)

#### NEW QUESTION 9

Which deployment model is the most secure when considering risks to cloud adoption?

- A. public cloud
- B. hybrid cloud
- C. community cloud
- D. private cloud

**Answer:** D

#### NEW QUESTION 10

What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

- A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
- B. It discovers and controls cloud apps that are connected to a company's corporate environment.
- C. It deletes any application that does not belong in the network.
- D. It sends the application information to an administrator to act on.

**Answer:** B

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features>

#### NEW QUESTION 10

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 11

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

- A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
- C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

**Answer:** B

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000>

## NEW QUESTION 12

### DRAG DROP

Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.

PortScan Detection	many-to-one PortScan in which multiple hosts query a single host for open ports
Port Sweep	one-to-one PortScan, attacker mixes spoofed source IP addresses with the actual scanning IP address
Decoy PortScan	one-to-many port sweep, an attacker against one or a few hosts to scan a single port on multiple target hosts
Distributed PortScan	one-to-one PortScan, an attacker against one or a few hosts to scan one or multiple ports

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting\\_specific\\_threats.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting_specific_threats.html)

## NEW QUESTION 17

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 20

In which cloud services model is the tenant responsible for virtual machine OS patching?

- A. IaaS
- B. UCaaS
- C. PaaS
- D. SaaS

**Answer:** A

### Explanation:

Reference: <https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php>

## NEW QUESTION 24

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](https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html)

## NEW QUESTION 29

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 34

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 39

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

**Answer:** BD

#### Explanation:

Reference: <https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf> chapter 2

#### NEW QUESTION 44

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 48

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 49

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 51

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 56

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 60

When wired 802.1X authentication is implemented, which two components are required? (Choose two.)

- A. authentication server: Cisco Identity Service Engine
- B. supplicant: Cisco AnyConnect ISE Posture module
- C. authenticator: Cisco Catalyst switch
- D. authenticator: Cisco Identity Services Engine
- E. authentication server: Cisco Prime Infrastructure

**Answer:** AC

#### Explanation:

Reference: <https://www.lookingpoint.com/blog/ise-series-802.1x>

#### NEW QUESTION 62

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

- A. Certificate Trust List
- B. Endpoint Trust List
- C. Enterprise Proxy Service
- D. Secured Collaboration Proxy

**Answer:** A

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html>

#### NEW QUESTION 63

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](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 66

Which two mechanisms are used to control phishing attacks? (Choose two.)

- A. Enable browser alerts for fraudulent websites.
- B. Define security group memberships.
- C. Revoke expired CRL of the websites.
- D. Use antispyware software.
- E. Implement email filtering techniques.

**Answer:** AE

#### NEW QUESTION 68

Which VPN technology can support a multivendor environment and secure traffic between sites?

- A. SSL VPN
- B. GET VPN
- C. FlexVPN
- D. DMVPN

**Answer:** C

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data\\_sheet\\_c78-704277.html](https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html)

#### NEW QUESTION 73

An MDM provides which two advantages to an organization with regards to device management? (Choose two.)

- A. asset inventory management
- B. allowed application management
- C. Active Directory group policy management
- D. network device management
- E. critical device management

**Answer:** AB

#### NEW QUESTION 78

Which Talos reputation center allows you to track the reputation of IP addresses for email and web traffic?

- A. IP Blacklist Center
- B. File Reputation Center
- C. AMP Reputation Center
- D. IP and Domain Reputation Center

**Answer:** D

#### NEW QUESTION 83

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

#### NEW QUESTION 85

Which solution combines Cisco IOS and IOS XE components to enable administrators to recognize applications, collect and send network metrics to Cisco Prime and other third-party management tools, and prioritize application traffic?

- A. Cisco Security Intelligence
- B. Cisco Application Visibility and Control
- C. Cisco Model Driven Telemetry
- D. Cisco DNA Center

**Answer:** B

#### NEW QUESTION 88

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 92

DRAG DROP

Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Install monitoring extension for AWS EC2.	step 1
Restart the Machine Agent.	step 2
Update config.yaml.	step 3
Configure a Machine Agent or SIM Agent.	step 4

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Configure a Machine Agent or SIM Agent.
Install monitoring extension for AWS EC2.
Update config.yaml.
Restart the Machine Agent.

#### NEW QUESTION 93

Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

- A. AMP
- B. AnyConnect
- C. DynDNS
- D. Talos

**Answer:** D

#### NEW QUESTION 96

What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

- A. It decrypts HTTPS application traffic for unauthenticated users.
- B. It alerts users when the WSA decrypts their traffic.
- C. It decrypts HTTPS application traffic for authenticated users.
- D. It provides enhanced HTTPS application detection for AsyncOS.

**Answer:** D

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user\\_guide/b\\_WSA\\_UserGuide\\_11\\_7/b\\_WSA\\_UserGuide\\_11\\_7\\_chapter\\_01011.html](https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html)

#### NEW QUESTION 97

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 98

What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

- A. Enable IP Layer enforcement.
- B. Activate the Advanced Malware Protection license
- C. Activate SSL decryption.
- D. Enable Intelligent Proxy.

**Answer:** D

#### NEW QUESTION 99

What is the primary difference between an Endpoint Protection Platform and an Endpoint Detection and Response?

- A. EPP focuses on prevention, and EDR focuses on advanced threats that evade perimeter defenses.
- B. EDR focuses on prevention, and EPP focuses on advanced threats that evade perimeter defenses.
- C. EPP focuses on network security, and EDR focuses on device security.
- D. EDR focuses on network security, and EPP focuses on device security.

**Answer:** A

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html>

#### NEW QUESTION 103

Which functions of an SDN architecture require southbound APIs to enable communication?

- A. SDN controller and the network elements
- B. management console and the SDN controller
- C. management console and the cloud
- D. SDN controller and the cloud

**Answer:** A

#### NEW QUESTION 105

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 108**

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 110**

What can be integrated with Cisco Threat Intelligence Director to provide information about security threats, which allows the SOC to proactively automate responses to those threats?

- A. Cisco Umbrella
- B. External Threat Feeds
- C. Cisco Threat Grid
- D. Cisco Stealthwatch

**Answer: C**

**NEW QUESTION 113**

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 114**

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](https://en.wikipedia.org/wiki/Buffer_overflow)

**NEW QUESTION 115**

An engineer must force an endpoint to re-authenticate an already authenticated session without disrupting the endpoint to apply a new or updated policy from ISE. Which CoA type achieves this goal?

- A. Port Bounce
- B. CoA Terminate
- C. CoA Reauth
- D. CoA Session Query

**Answer: C**

**NEW QUESTION 118**

Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two.)

- A. SIP
- B. inline normalization
- C. SSL
- D. packet decoder
- E. modbus

**Answer: AC**

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application\\_Layer\\_Preprocessors.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html)

**NEW QUESTION 122**

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 126

The main function of northbound APIs in the SDN architecture is to enable communication between which two areas of a network?

- A. SDN controller and the cloud
- B. management console and the SDN controller
- C. management console and the cloud
- D. SDN controller and the management solution

**Answer:** D

#### NEW QUESTION 129

What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

- A. It tracks flow-create, flow-teardown, and flow-denied events.
- B. It provides stateless IP flow tracking that exports all records of a specific flow.
- C. It tracks the flow continuously and provides updates every 10 seconds.
- D. Its events match all traffic classes in parallel.

**Answer:** A

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nse1.html>

#### NEW QUESTION 130

.....

## 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