

# Cisco

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



#### NEW QUESTION 1

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 2

Refer to the exhibit.

Interface	MAC Address	Method	Domain	Status	Fq Session ID
Gi4/15	0050.b6d4.8a60	dot1x	DATA	Auth	0A02198200001
Gi8/43	0024.c4fe.1832	dot1x	VOICE	Auth	0A02198200000
Gi10/25	0026.7391.bbd1	dot1x	DATA	Auth	0A02198200001
Gi8/28	0026.0b5e.51d5	dot1x	VOICE	Auth	0A02198200000
Gi4/13	0025.4593.e575	dot1x	VOICE	Auth	0A02198200000
Gi10/23	0025.8418.217f	dot1x	VOICE	Auth	0A02198200000
Gi7/4	0025.8418.1bc7	dot1x	VOICE	Auth	0A02198200000
Gi7/7	0026.0b5e.50fb	dot1x	VOICE	Auth	0A02198200000
Gi8/14	c85b.7604.fa1d	dot1x	DATA	Auth	0A02198200001
Gi10/29	0026.0b5e.528a	dot1x	VOICE	Auth	0A02198200000
Gi4/2	0026.0b5e.4f9f	dot1x	VOICE	Auth	0A02198200000
Gi10/30	0025.4593.e5ac	dot1x	VOICE	Auth	0A02198200000
Gi8/29	68bd.aba5.2e44	dot1x	VOICE	Auth	0A02198200001
Gi7/4	54ee.75db.d766	dot1x	DATA	Auth	0A02198200001
Gi2/34	e804.62eb.a658	dot1x	VOICE	Auth	0A02198200000
Gi10/22	482a.e307.d9c8	dot1x	DATA	Auth	0A02198200001
Gi9/22	0007.b00c.8c35	mab	DATA	Auth	0A02198200000

Which command was used to generate this output and to show which ports are authenticating with dot1x or mab?

- A. show authentication registrations
- B. show authentication method
- C. show dot1x all
- D. show authentication sessions

**Answer:** B

#### NEW QUESTION 3

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 4

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 5

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 6**

Which exfiltration method does an attacker use to hide and encode data inside DNS requests and queries?

- A. DNS tunneling
- B. DNSCrypt
- C. DNS security
- D. DNSSEC

**Answer:** A

**Explanation:**

Reference: <https://learn-umbrella.cisco.com/cloud-security/dns-tunneling>

**NEW QUESTION 7**

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 8**

Which two probes are configured to gather attributes of connected endpoints using Cisco Identity Services Engine? (Choose two.)

- A. RADIUS
- B. TACACS+
- C. DHCP
- D. sFlow
- E. SMTP

**Answer:** AC

**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 9**

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 10**

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 10

Which two key and block sizes are valid for AES? (Choose two.)

- A. 64-bit block size, 112-bit key length  
 B. 64-bit block size, 168-bit key length  
 C. 128-bit block size, 192-bit key length  
 D. 128-bit block size, 256-bit key length  
 E. 192-bit block size, 256-bit key length

**Answer:** CD

**Explanation:**

Reference: [https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

#### NEW QUESTION 11

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

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

**Answer:** A

#### NEW QUESTION 16

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 18

What is a language format designed to exchange threat intelligence that can be transported over the TAXII protocol?

- A. STIX
- B. XMPP
- C. pxGrid
- D. SMTP

**Answer:** A

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/security/web\\_security/scancenter/administrator/guide/b\\_ScanCenter\\_Administrator\\_Guide/b\\_ScanCenter\\_Administrator\\_Guide\\_chapter\\_0100011.pdf](https://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_0100011.pdf)

#### NEW QUESTION 19

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 24

What is a characteristic of Dynamic ARP Inspection?

- A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.
- B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.
- C. DAI associates a trust state with each switch.
- D. DAI intercepts all ARP requests and responses on trusted ports only.

**Answer:** A

#### NEW QUESTION 25

DRAG DROP

Drag and drop the descriptions from the left onto the correct protocol versions on the right.

[MISSING]

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

[MISSING]

#### NEW QUESTION 29

Which statement about IOS zone-based firewalls is true?

- A. An unassigned interface can communicate with assigned interfaces
- B. Only one interface can be assigned to a zone.
- C. An interface can be assigned to multiple zones.
- D. An interface can be assigned only to one zone.

**Answer:** D

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>

#### NEW QUESTION 32

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 34

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 38

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 42

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 45

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 49

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 53

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 56

Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

- A. Patch for cross-site scripting.
- B. Perform backups to the private cloud.
- C. Protect against input validation and character escapes in the endpoint.



- D. Install a spam and virus email filter.
- E. Protect systems with an up-to-date antimalware program.

**Answer:** DE

**NEW QUESTION 61**

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 64**

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 68**

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 70**

On which part of the IT environment does DevSecOps focus?

- A. application development
- B. wireless network
- C. data center
- D. perimeter network

**Answer:** A

**NEW QUESTION 75**

In a PaaS model, which layer is the tenant responsible for maintaining and patching?

- A. hypervisor
- B. virtual machine
- C. network
- D. application

**Answer:** D

**Explanation:**

Reference: <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>

**NEW QUESTION 77**

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 81**

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

**NEW QUESTION 86**

How does Cisco Stealthwatch Cloud provide security for cloud environments?

- A. It delivers visibility and threat detection.
- B. It prevents exfiltration of sensitive data.
- C. It assigns Internet-based DNS protection for clients and servers.
- D. It facilitates secure connectivity between public and private networks.

**Answer:** A

**Explanation:**

<https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/FBLP/Cisco/Cisco-091919-Simple-IT-Whitepaper.pdf>

**NEW QUESTION 89**

Refer to the exhibit.

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

S*  0.0.0.0 0.0.0.0 [1/0] via 1.1.1.1, outside
C    1.1.1.0 255.255.255.0 is directly connect, outside
S    172.16.0.0 255.255.0.0 [1/0] via 192.168.100.1, inside
C    192.168.100.0 255.255.255.0 is directly connected, inside
C    172.16.10.0 255.255.255.0 is directly connected, dmz
S    10.10.10.0 255.255.255.0 [1/0] via 172.16.10.1, dmz

access-list redirect-acl permit ip 192.168.100.0 255.255.255.0 any
access-list redirect-acl permit ip 172.16.0.0 255.255.0.0 any

class-map redirect-class
 match access-list redirect-acl

policy-map inside-policy
 class redirect-class
  sfr fail-open

service-policy inside-policy global
```

What is a result of the configuration?

- A. Traffic from the DMZ network is redirected.
- B. Traffic from the inside network is redirected.
- C. All TCP traffic is redirected.
- D. Traffic from the inside and DMZ networks is redirected.

**Answer:** D

**NEW QUESTION 92**

Which information is required when adding a device to Firepower Management Center?

- A. username and password
- B. encryption method
- C. device serial number
- D. registration key

**Answer:** D

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device\\_Management\\_Basics.html#ID-2242-0000069d](https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-0000069d)

**NEW QUESTION 95**

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 98**

.....

## 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](#)**