

# Cisco

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies



#### 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

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 3

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 4

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 5

Refer to the exhibit.

Interface	MAC Address	Method	Domain	Status	Fg 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 6**

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

- A. SAT
- B. BAT
- C. HAT
- D. RAT

**Answer:** D

**NEW QUESTION 7**

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

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

**Answer:** BC

**NEW QUESTION 8**

Which policy represents a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in a deployment?

- A. group policy
- B. access control policy
- C. device management policy
- D. platform service policy

**Answer:** D

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/platform\\_settings\\_policies\\_for\\_managed\\_devices.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/platform_settings_policies_for_managed_devices.pdf)

**NEW QUESTION 9**

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 10**

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 10**

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 12

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 13

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 14

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 17

What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

- A. biometric factor
- B. time factor
- C. confidentiality factor
- D. knowledge factor
- E. encryption factor

**Answer:** AD

#### NEW QUESTION 18

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 21

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 23

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 27

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 28

What is the function of Cisco Cloudlock for data security?

- A. data loss prevention
- B. controls malicious cloud apps
- C. detects anomalies
- D. user and entity behavior analytics

**Answer:** A

**Explanation:**

Reference: <https://umbrella.cisco.com/products/casb>

#### NEW QUESTION 31

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 35

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 37

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 42

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 47

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 52

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 57

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 61

Which two behavioral patterns characterize a ping of death attack? (Choose two.)

- A. The attack is fragmented into groups of 16 octets before transmission.
- B. The attack is fragmented into groups of 8 octets before transmission.
- C. Short synchronized bursts of traffic are used to disrupt TCP connections.
- D. Malformed packets are used to crash systems.
- E. Publicly accessible DNS servers are typically used to execute the attack.

**Answer:** BD

#### Explanation:

Reference: [https://en.wikipedia.org/wiki/Ping\\_of\\_death](https://en.wikipedia.org/wiki/Ping_of_death)

#### NEW QUESTION 64

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 66

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 69

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 71

Why would a user choose an on-premises ESA versus the CES solution?

- A. Sensitive data must remain onsite.
- B. Demand is unpredictable.
- C. The server team wants to outsource this service.
- D. ESA is deployed inline.

**Answer:** A

#### NEW QUESTION 74

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 76

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 77

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 81

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 86

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 87

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 91

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 95

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 96

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 98

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 101

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 104

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 107

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 112**

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 113**

.....

## 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](#)**