

## Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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



#### 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

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

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

**Answer:** BC

#### NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

Which network monitoring solution uses streams and pushes operational data to provide a near real-time view of activity?

- A. SNMP
- B. SMTP
- C. syslog
- D. model-driven telemetry

**Answer:** D

**Explanation:**

Reference: <https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide>

#### 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

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 10

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 11

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 16

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

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

**Answer:** A

#### NEW QUESTION 19

Which statement about the configuration of Cisco ASA NetFlow v9 Secure Event Logging is true?

- A. To view bandwidth usage for NetFlow records, the QoS feature must be enabled.
- B. A sysopt command can be used to enable NSEL on a specific interface.
- C. NSEL can be used without a collector configured.
- D. A flow-export event type must be defined under a policy.

**Answer:** D

#### NEW QUESTION 20

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 24

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 26

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 34**

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\\_chapter\\_00.pdf](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_chapter_00.pdf)

**NEW QUESTION 36**

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 41**

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 45**

Which SNMPv3 configuration must be used to support the strongest security possible?

- A. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv des ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- B. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- C. asa-host(config)#snmp-server group myv3 v3 noauth asa-host(config)#snmp-server user andy myv3 auth sha cisco priv 3des ciscXXXXXXXXXasa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy
- D. asa-host(config)#snmp-server group myv3 v3 priv asa-host(config)#snmp-server user andy myv3 auth sha cisco priv aes 256 ciscXXXXXXXXX asa-host(config)#snmp-server host inside 10.255.254.1 version 3 andy

**Answer:** D

**NEW QUESTION 49**

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 52**

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 54

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 57

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 61

Which two features of Cisco DNA Center are used in a Software Defined Network solution? (Choose two.)

- A. accounting
- B. assurance
- C. automation
- D. authentication
- E. encryption

**Answer:** BC

#### Explanation:

Reference: <https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html>

#### NEW QUESTION 63

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 66

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 67

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 68

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 72

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

An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

- A. device flow correlation
- B. simple detections
- C. application blocking list
- D. advanced custom detections

**Answer:** C

#### NEW QUESTION 78

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 82

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 87

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 92

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

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 100

Refer to the exhibit.

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet1/0/12
-----
PAE                  = AUTHENTICATOR
PortControl          = FORCE_AUTHORIZED
ControlDirection     = Both
HostMode              = SINGLE_HOST
QuietPeriod          = 60
ServerTimeout         = 0
SuppTimeout          = 30
ReAuthMax             = 2
MaxReq                = 2
TxPeriod              = 30
```

Which command was used to display this output?

- A. show dot1x all
- B. show dot1x
- C. show dot1x all summary
- D. show dot1x interface gi1/0/12

**Answer:** A

#### Explanation:

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html)

#### NEW QUESTION 103

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 104

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 105

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 110

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 112

Which two services must remain as on-premises equipment when a hybrid email solution is deployed? (Choose two.)

- A. DDoS
- B. antispam
- C. antivirus
- D. encryption
- E. DLP

**Answer:** DE

#### Explanation:

Reference: [https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview\\_guide/Cisco\\_Cloud\\_Hybrid\\_Email\\_Security\\_Overview\\_Guide.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf)

#### NEW QUESTION 114

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 118

Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

- A. phishing

- B. brute force
- C. man-in-the-middle
- D. DDOS
- E. tear drop

**Answer:** BC

#### NEW QUESTION 122

.....

## 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