

Exam Questions 350-701

Implementing and Operating Cisco Security Core Technologies

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



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

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 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

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

NEW QUESTION 6

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

NEW QUESTION 7

Which two conditions are prerequisites for stateful failover for IPsec? (Choose two.)

- A. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically.
- B. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
- C. The IPsec configuration that is set up on the active device must be duplicated on the standby device.
- D. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
- E. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device.

Answer: BC

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpn-availability-15-mt-book/sec-state-fail-ipsec.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

NEW QUESTION 9

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 10

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 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 14

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 18

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

NEW QUESTION 19

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

NEW QUESTION 20

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 21

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 23

Which command enables 802.1X globally on a Cisco switch?

- A. dot1x system-auth-control
- B. dot1x pae authenticator

- C. authentication port-control auto
- D. aaa new-model

Answer: A

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/routers/nfvis/switch_command/b-nfvis-switch-command-reference/802_1x_commands.html

NEW QUESTION 27

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 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 35

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 36

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 41

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

NEW QUESTION 46

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 antispam software.
- E. Implement email filtering techniques.

Answer: AE

NEW QUESTION 51

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 56

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 59

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 63

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 67

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 70

Which cloud service model offers an environment for cloud consumers to develop and deploy applications without needing to manage or maintain the underlying cloud infrastructure?

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

Answer: A

NEW QUESTION 71

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 73

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 74

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 77

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 82

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 83

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 85

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 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 90

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

NEW QUESTION 91

.....

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