



350-701^{Q&As}

Implementing and Operating Cisco Security Core Technologies (SCOR)

Pass Cisco 350-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/350-701.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

What is the role of an endpoint in protecting a user from a phishing attack?

- A. Use Cisco Stealthwatch and Cisco ISE Integration.
- B. Utilize 802.1X network security to ensure unauthorized access to resources.
- C. Use machine learning models to help identify anomalies and determine expected sending behavior.
- D. Ensure that antivirus and anti malware software is up to date

Correct Answer: C

QUESTION 2

An organization uses Cisco FMC to centrally manage multiple Cisco FTD devices. The default management port conflicts with other communications on the network and must be changed. What must be done to ensure that all devices can communicate together?

- A. Manually change the management port on Cisco FMC and all managed Cisco FTD devices
- B. Set the tunnel to go through the Cisco FTD
- C. Change the management port on Cisco FMC so that it pushes the change to all managed Cisco FTD devices
- D. Set the tunnel port to 8305

Correct Answer: A

: The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305. Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate with each other. Reference: <https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmtnw.html>

QUESTION 3

Refer to the exhibit.



```
Info: New SMTP ICID 30 interface Management (192.168.0.100)
      address 10.128.128.200 reverse dns host unknown verified no
Info: ICID 30 ACCEPT SG SUSPECTLIST match sbrs[none] SBRs None
Info: ICID 30 TLS success protocol TLSv1 cipher
      DHE-RSA-AES256-SHA
Info: SMTP Auth: (ICID 30) succeeded for user: cisco using
      AUTH mechanism: LOGIN with profile: ldap_smtp
Info: MID 80 matched all recipients for per-recipient policy
      DEFAULT in the outbound table
```

Which type of authentication is in use?

- A. LDAP authentication for Microsoft Outlook
- B. POP3 authentication
- C. SMTP relay server authentication
- D. external user and relay mail authentication

Correct Answer: D

Reference: <https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technoteesa-00.html>
The exhibit in this Question shows a successful TLS connection from the remote host (reception) in the mail log.

QUESTION 4

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

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

Correct Answer: C

FlexVPN is an IKEv2-based VPN technology that provides several benefits beyond traditional site-to-site VPN implementations. FlexVPN is a standards-based solution that can interoperate with non-Cisco IKEv2 implementations. Therefore FlexVPN can support a multivendor environment. All of the three VPN technologies support traffic between sites (site-to-site or spoke-to-spoke).

QUESTION 5

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.

Correct Answer: A

QUESTION 6

What must be used to share data between multiple security products?

- A. Cisco Rapid Threat Containment
- B. Cisco Platform Exchange Grid
- C. Cisco Advanced Malware Protection
- D. Cisco Stealthwatch Cloud

Correct Answer: B

QUESTION 7

A network engineer is configuring DMVPN and entered the crypto isakmp key cisc0380739941 address 0.0.0.0 command on host A. The tunnel is not being established to host B. What action is needed to authenticate the VPN?

- A. Enter the same command on host B.
- B. Enter the command with a different password on host B.
- C. Change isakmp to ikev2 in the command on host A.
- D. Change the password on host A to the default password.

Correct Answer: A

QUESTION 8

What is the purpose of the My Devices Portal in a Cisco ISE environment?

- A. to register new laptops and mobile devices
- B. to request a newly provisioned mobile device
- C. to provision userless and agentless systems
- D. to manage and deploy antivirus definitions and patches on systems owned by the end user



Correct Answer: A

Reference: https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/mydevices/b_mydevices_2x.html

QUESTION 9

What is a commonality between DMVPN and FlexVPN technologies?

- A. FlexVPN and DMVPN use IS-IS routing protocol to communicate with spokes
- B. FlexVPN and DMVPN use the new key management protocol
- C. FlexVPN and DMVPN use the same hashing algorithms
- D. IOS routers run the same NHRP code for DMVPN and FlexVPN

Correct Answer: D

Reference: <https://packetpushers.net/cisco-flexvpn-dmvpn-high-level-design/>

QUESTION 10

An administrator configures a Cisco WSA to receive redirected traffic over ports 80 and 443. The organization requires that a network device with specific WSA integration capabilities be configured to send the traffic to the WSA to proxy the requests and increase visibility, while making this invisible to the users. What must be done on the Cisco WSA to support these requirements?

- A. Configure transparent traffic redirection using WCCP in the Cisco WSA and on the network device
- B. Configure active traffic redirection using WPAD in the Cisco WSA and on the network device
- C. Use the Layer 4 setting in the Cisco WSA to receive explicit forward requests from the network device
- D. Use PAC keys to allow only the required network devices to send the traffic to the Cisco WSA

Correct Answer: A

QUESTION 11

Which attack is commonly associated with C and C++ programming languages?

- A. cross-site scripting
- B. water holing
- C. DDoS
- D. buffer overflow

Correct Answer: D



A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Buffer overflow is a vulnerability in low level codes of C and C++. An attacker can cause the program to crash, make data corrupt, steal some private information or run his/her own code. It basically means to access any buffer outside of it's allotted memory space. This happens quite frequently in the case of arrays.

QUESTION 12

Which option is the main function of Cisco Firepower impact flags?

- A. They alert administrators when critical events occur.
- B. They highlight known and suspected malicious IP addresses in reports.
- C. They correlate data about intrusions and vulnerability.
- D. They identify data that the ASA sends to the Firepower module.

Correct Answer: C

QUESTION 13

An engineer wants to generate NetFlow records on traffic traversing the Cisco ASA. Which Cisco ASA command must be used?

- A. flow-export destination inside 1.1.1.1 2055
- B. ip flow monitor input
- C. ip flow-export destination 1.1.1.1 2055
- D. flow exporter

Correct Answer: A

Reference:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_c onfig/monitor_nsel.html

QUESTION 14

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



Correct Answer: A

QUESTION 15

What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

- A. show authorization status
- B. show authen sess int gi0/1
- C. show connection status gi0/1
- D. show ver gi0/1

Correct Answer: B

[350-701 VCE Dumps](#)

[350-701 Practice Test](#)

[350-701 Exam Questions](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

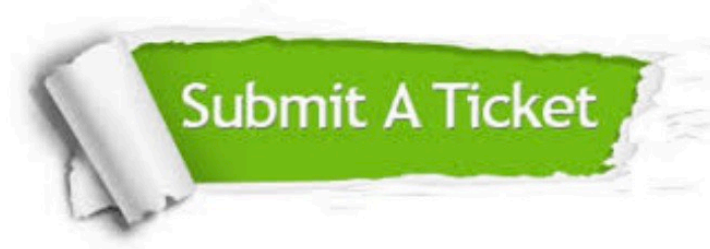
- 100% Guaranteed Success
- 100% Money Back Guarantee
- 365 Days Free Update
- Instant Download After Purchase
- 24x7 Customer Support
- Average 99.9% Success Rate
- More than 800,000 Satisfied Customers Worldwide
- Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.passapply.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © passapply, All Rights Reserved.