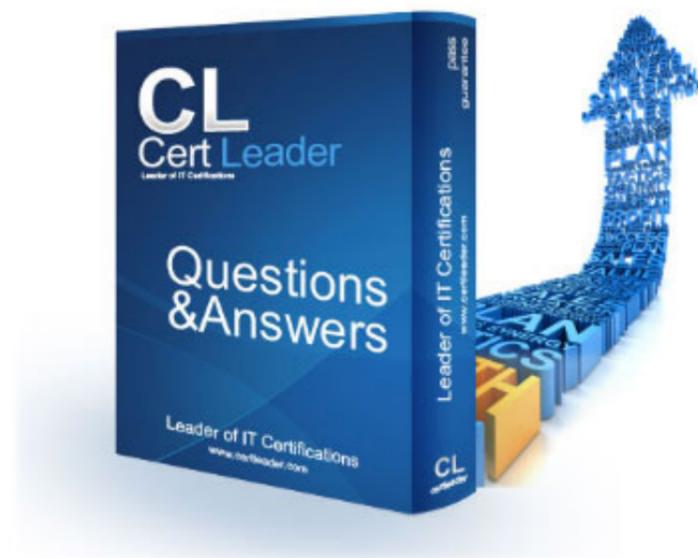


350-701 Dumps

Implementing and Operating Cisco Security Core Technologies

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



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 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 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_011110.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

NEW QUESTION 7

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 8

How does Cisco Umbrella archive logs to an enterprise- owned storage?

- A. by using the Application Programming Interface to fetch the logs
- B. by sending logs via syslog to an on-premises or cloud-based syslog server
- C. by the system administrator downloading the logs from the Cisco Umbrella web portal
- D. by being configured to send logs to a self-managed AWS S3 bucket

Answer: D

Explanation:

Reference: <https://docs.umbrella.com/deployment-umbrella/docs/log-management>

NEW QUESTION 9

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 10

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

NEW QUESTION 10

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 14

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 19

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 24

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 27

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 31

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 32

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 36

Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

- A. transparent
- B. redirection
- C. forward
- D. proxy gateway

Answer: A

Explanation:

Reference: <https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/117940-qa-wsa-00.html>

NEW QUESTION 38

An MDM provides which two advantages to an organization with regards to device management? (Choose two.)

- A. asset inventory management
- B. allowed application management
- C. Active Directory group policy management
- D. network device management
- E. critical device management

Answer: AB

NEW QUESTION 40

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 45

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 49

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 54

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 55

What is the purpose of the Decrypt for Application Detection feature within the WSA Decryption options?

- A. It decrypts HTTPS application traffic for unauthenticated users.
- B. It alerts users when the WSA decrypts their traffic.
- C. It decrypts HTTPS application traffic for authenticated users.

D. It provides enhanced HTTPS application detection for AsyncOS.

Answer: D

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01011.html

NEW QUESTION 57

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 58

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 62

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 65

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 70

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 75

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 76

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

NEW QUESTION 77

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 80

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

NEW QUESTION 81

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 84

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 87

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

NEW QUESTION 91

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 96

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 350-701 Exam with Our Prep Materials Via below:

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