

## 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**

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 3**

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](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 4**

Which deployment model is the most secure when considering risks to cloud adoption?

- A. public cloud
- B. hybrid cloud
- C. community cloud
- D. private cloud

**Answer:** D

**NEW QUESTION 5**

What is the result of running the crypto isakmp key ciscXXXXXXXX address 172.16.0.0 command?

- A. authenticates the IKEv2 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- B. authenticates the IP address of the 172.16.0.0/32 peer by using the key ciscXXXXXXXX
- C. authenticates the IKEv1 peers in the 172.16.0.0/16 range by using the key ciscXXXXXXXX
- D. secures all the certificates in the IKE exchange by using the key ciscXXXXXXXX

**Answer:** B

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c4.html#wp6039879000>

**NEW QUESTION 6**

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 7**

Where are individual sites specified to be blacklisted in Cisco Umbrella?

- A. application settings
- B. content categories
- C. security settings
- D. destination lists

**Answer:** D

**NEW QUESTION 8**

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 9**

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 10**

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 10**

Under which two circumstances is a CoA issued? (Choose two.)

- A. A new authentication rule was added to the policy on the Policy Service node.
- B. An endpoint is deleted on the Identity Service Engine server.
- C. A new Identity Source Sequence is created and referenced in the authentication policy.
- D. An endpoint is profiled for the first time.
- E. A new Identity Service Engine server is added to the deployment with the Administration persona.

**Answer:** BD

**Explanation:**

Reference: [https://www.cisco.com/en/US/docs/security/ise/1.0/user\\_guide/ise10\\_prof\\_pol.html](https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html)

**NEW QUESTION 14**

Which two features are used to configure Cisco ESA with a multilayer approach to fight viruses and malware? (Choose two.)

- A. Sophos engine
- B. white list
- C. RAT
- D. outbreak filters
- E. DLP

**Answer:** AD

**NEW QUESTION 19**

How is Cisco Umbrella configured to log only security events?

- A. per policy
- B. in the Reporting settings
- C. in the Security Settings section
- D. per network in the Deployments section

**Answer:** A

**Explanation:**

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

**NEW QUESTION 21**

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 23**

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 24**

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 25**

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 28**

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 33**

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 37

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 38

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 41

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 46

.....

## 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>