

## 350-701 Dumps

# Implementing and Operating Cisco Security Core Technologies

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



**NEW QUESTION 1**

Which policy is used to capture host information on the Cisco Firepower Next Generation Intrusion Prevention System?

- A. correlation
- B. intrusion
- C. access control
- D. network discovery

**Answer: D**

**NEW QUESTION 2**

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 3**

An engineer is configuring a Cisco ESA and wants to control whether to accept or reject email messages to a recipient address. Which list contains the allowed recipient addresses?

- A. SAT
- B. BAT
- C. HAT
- D. RAT

**Answer: D**

**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](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**

In which form of attack is alternate encoding, such as hexadecimal representation, most often observed?

- A. smurf
- B. distributed denial of service
- C. cross-site scripting
- D. rootkit exploit

**Answer: C**

**NEW QUESTION 6**

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 7**

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 8**

What does the Cloudlock Apps Firewall do to mitigate security concerns from an application perspective?

- A. It allows the administrator to quarantine malicious files so that the application can function, just not maliciously.
- B. It discovers and controls cloud apps that are connected to a company's corporate environment.
- C. It deletes any application that does not belong in the network.
- D. It sends the application information to an administrator to act on.

**Answer:** B

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/products/security/cloudlock/index.html#~features>

**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**

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 14**

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 15**

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 18**

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 21**

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 23**

DRAG DROP

Drag and drop the capabilities from the left onto the correct technologies on the right.

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks	Next Generation Intrusion Prevention System
superior threat prevention and mitigation for known and unknown threats	Advanced Malware Protection
application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs	application control and URL filtering
combined integrated solution of strong defense and web protection, visibility, and controlling solutions	Cisco Web Security Appliance

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

superior threat prevention and mitigation for known and unknown threats

superior threat prevention and mitigation for known and unknown threats

detection, blocking, tracking, analysis, and remediation to protect against targeted persistent malware attacks

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

application-layer control and ability to enforce usage and tailor detection policies based on custom applications and URLs

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

combined integrated solution of strong defense and web protection, visibility, and controlling solutions

**NEW QUESTION 26**

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](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

**NEW QUESTION 30**

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 34**

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 36**

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 41**

What are two list types within AMP for Endpoints Outbreak Control? (Choose two.)

- A. blocked ports
- B. simple custom detections
- C. command and control
- D. allowed applications
- E. URL

**Answer:** BD

**Explanation:**

Reference: <https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20User%20Guide.pdf> chapter 2

**NEW QUESTION 44**

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 45**

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\\_1\\_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_1_chapter_00.pdf)

**NEW QUESTION 47**

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 48**

The Cisco ASA must support TLS proxy for encrypted Cisco Unified Communications traffic. Where must the ASA be added on the Cisco UC Manager platform?

- A. Certificate Trust List
- B. Endpoint Trust List
- C. Enterprise Proxy Service
- D. Secured Collaboration Proxy

**Answer:** A

**Explanation:**

Reference: <https://www.cisco.com/c/en/us/td/docs/security/asa/special/unified-communications/guide/unified-comm/unified-comm-tlsproxy.html>

**NEW QUESTION 52**

Which API is used for Content Security?

- A. NX-OS API
- B. IOS XR API
- C. OpenVuln API
- D. AsyncOS API

**Answer:** D

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/td/docs/security/security\\_management/sma/sma12-0/api/b\\_SMA\\_API\\_12/test\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma12-0/api/b_SMA_API_12/test_chapter_01.html)

**NEW QUESTION 54**

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 56**

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

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

**Answer: C**

**Explanation:**

Reference: [https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data\\_sheet\\_c78-704277.html](https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html)

**NEW QUESTION 58**

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 61**

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 62**

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 67**

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 68**

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 73**

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 77**

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 82**

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 84**

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 88**

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 89**

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 94**

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 95**

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 99**

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 100**

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 101**

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 104**

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 109**

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 110**

.....

## 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>