350-701.premium.102q - DEMO

Number: 350-701
Passing Score: 800
Time Limit: 120 min

350-701

Implementing and Operating Cisco Security Core Technologies

Exam A

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

```
aaa new-model

radius-server host 10.0.0.12 key secret12
```

Refer to the exhibit. 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 Which two preventive measures are used to control cross-site scripting?
(Choose two.)

A. Enable client-side scripts on a per-domain basis.
B. Incorporate contextual output encoding/escaping.
C. Disable cookie inspection in the HTML inspection engine.
D. Run untrusted HTML input through an HTML sanitization engine.
E. SameSite cookie attribute should not be used.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

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

Refer to the exhibit. 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**

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 7 Which two capabilities does TAXII support?
(Choose two.)

A. exchange
B. pull messaging
C. binding
D. correlation
E. mitigating

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 9
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 10 What are two Detection and Analytics Engines of Cognitive Threat
Analytics? (Choose two.)

A. data exfiltration
B. command and control communication

C. intelligent proxy
D. snort
E. URL categorization

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-a-glance-c45-736555.pdf

QUESTION 11 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 13
When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.umbrella.com/hc/en-us/articles/115004563666-Understanding-Security-Categories

QUESTION 14
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

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
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_01110.html

QUESTION 15 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://tools.cisco.com/security/center/resources/sql_injection

QUESTION 16 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 18 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://learn-umbrella.cisco.com/cloud-security/dns-tunneling

QUESTION 19 Which algorithm provides encryption and authentication for data plane communication?

A. AES-GCM
B. SHA-96
C. AES-256D. SHA-384

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/products/collateral/security/cloudlock/cisco-cloudlock-cloud-data-security-datasheet.pdf

QUESTION 21

```
snmp-server group SNMP v3 auth access 15
```

Refer to the exhibit. 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide

QUESTION 23
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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 24 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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

QUESTION 25
DRAG DROP

Drag and drop the Firepower Next Generation Intrustion Prevention System detectors from the left onto the correct definitions on the right.

Select and Place:
Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/detecting_specific_threats.html

QUESTION 26 Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus
B. Stealthwatch
C. Firepower
D. Tetration

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/index.html#~products

QUESTION 27 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
DRAG DROP

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

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 29 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 lengthD. 128-bit block size, 256-bit key length
E. 192-bit block size, 256-bit key length

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

QUESTION 30 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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 31 In which cloud services model is the tenant responsible for virtual machine OS patching?

A. IaaS
B. UCaaS
C. PaaS
D. SaaS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cmswire.com/cms/information-management/cloud-service-models-iaas-saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

QUESTION 32 Which two descriptions of AES encryption are true? (Choose two.)

A. AES is less secure than 3DES.
B. AES is more secure than 3DES.
C. AES can use a 168-bit key for encryption.
D. AES can use a 256-bit key for encryption.
E. AES encrypts and decrypts a key three times in sequence.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://gpdb.docs.pivotal.io/43190/admin_guide/topics/ipsec.html

QUESTION 33 Which technology is used to improve web traffic performance by proxy caching?

A. WSA
B. Firepower
C. FireSIGHT
D. ASA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35 Which benefit does endpoint security provide the overall security posture of an organization?

A. It streamlines the incident response process to automatically perform digital forensics on the endpoint.
B. It allows the organization to mitigate web-based attacks as long as the user is active in the domain.
C. It allows the organization to detect and respond to threats at the edge of the network.
D. It allows the organization to detect and mitigate threats that the perimeter security devices do not detect.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 38 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

Correct Answer: BD
Section: (none)
Explanation

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

QUESTION 39 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**

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 40 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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://umbrella.cisco.com/products/casb

QUESTION 41 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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 What is a characteristic of Dynamic ARP Inspection?

A. DAI determines the validity of an ARP packet based on valid IP to MAC address bindings from the DHCP snooping binding database.
B. In a typical network, make all ports as trusted except for the ports connecting to switches, which are untrusted.
C. DAI associates a trust state with each switch.
D. DAI intercepts all ARP requests and responses on trusted ports only.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43 Which Cisco product provides proactive endpoint protection and allows administrators to centrally manage the deployment?

A. NGFW
B. AMP
C. WSA
D. ESA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
DRAG DROP

Drag and drop the descriptions from the left onto the correct protocol versions on the right.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 45 Where are individual sites specified to be blacklisted in Cisco Umbrella?

A. application settings
B. content categories
C. security settingsD. destination lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Which statement about IOS zone-based firewalls is true?

A. An unassigned interface can communicate with assigned interfaces
B. Only one interface can be assigned to a zone.
C. An interface can be assigned to multiple zones.
D. An interface can be assigned only to one zone.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

QUESTION 47 Which two activities can be done using Cisco DNA Center? (Choose two.)

A. DHCP
B. design
C. accounting
D. DNS
E. provision

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
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_chapter_00.pdf

QUESTION 48 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 How is ICMP used an exfiltration technique?

A. by flooding the destination host with unreachable packets
B. by sending large numbers of ICMP packets with a targeted hosts 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 hostD. by overwhelming a targeted host with ICMP echo-request packets

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 What is the difference between deceptive phishing and spear phishing?

A. Deceptive phishing is an attacked 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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
When wired 802.1X authentication is implemented, which two components are required? (Choose two.)
A. authentication server: Cisco Identity Service Engine
B. supplicant: Cisco AnyConnect ISE Posture module
C. authenticator: Cisco Catalyst switch
D. authenticator: Cisco Identity Services Engine

E. authentication server: Cisco Prime Infrastructure

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.lookingpoint.com/blog/ise-series-802.1x

QUESTION 53
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 54 Which API is used for
Content Security?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 55 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Ping_of_death

QUESTION 56 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 antispyware software.
E. Implement email filtering techniques.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57 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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/data_sheet_c78-704277.html

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 ciscXXXXXXXX** 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 ciscXXXXXXXX** 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 ciscXXXXXXXX**
asa-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 ciscXXXXXXXX** asa-host(config)#**snmp-server host inside 10.255.254.1 version 3 andy**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start-book/asav-96-qsg/asav-aws.html

QUESTION 60 Which proxy mode must be used on Cisco WSA to redirect TCP traffic with WCCP?

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

Correct Answer: A
Section: (none)
Explanation

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

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 63 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.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

QUESTION 64 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
DRAG DROP

Drag and drop the steps from the left into the correct order on the right to enable AppDynamics to monitor an EC2 instance in Amazon Web Services.

Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:

QUESTION 68 Why would a user choose an on-premises ESA versus the CES solution?

A. Sensitive data must remain onsite.
B. Demand is unpredictable.
C. The server team wants to outsource this service.
D. ESA is deployed inline.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70 Which Cisco solution does Cisco Umbrella integrate with to determine if a URL is malicious?

A. AMP
B. AnyConnect
C. DynDNS
D. Talos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 72 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73 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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

QUESTION 74
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75 What is a required prerequisite to enable malware file scanning for the Secure Internet Gateway?

A. Enable IP Layer enforcement.
B. Activate the Advanced Malware Protection license
C. Activate SSL decryption.
D. Enable Intelligent Proxy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76 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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77 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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 78
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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr.html

QUESTION 79 On which part of the IT environment does DevSecOps focus?

A. application development
B. wireless network
C. data center
D. perimeter network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80 Which functions of an SDN architecture require southbound APIs to enable communication?

A. SDN controller and the network elements
B. management console and the SDN controller
C. management console and the cloud
D. SDN controller and the cloud

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81 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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/12-1E/configuration/guide/storm.html

QUESTION 82 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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/api/qsg-asa-api.html

QUESTION 83 In a PaaS model, which layer is the tenant responsible for maintaining and patching?

A. hypervisor
B. virtual machine
C. network
D. application

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

QUESTION 84
An engineer is configuring AMP for endpoints and wants to block certain files from executing. Which outbreak control method is used to accomplish this task?

A. device flow correlation
B. simple detections
C. application blocking list
D. advanced custom detections

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 86 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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/white-paper-c11-740505.html

QUESTION 87
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88 What provides visibility and awareness into what is currently occurring on the network?

A. CMX
B. WMI
C. Prime Infrastructure
D. Telemetry

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89 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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Buffer_overflow

QUESTION 90 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91

```
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
```


Refer to the exhibit. 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**

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 92
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.

Correct Answer: AB

Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/SQL_injection

QUESTION 93 How does Cisco Stealthwatch Cloud provide security for cloud environments?

A. It delivers visibility and threat detection.
B. It prevents exfiltration of sensitive data.
C. It assigns Internet-based DNS protection for clients and servers.
D. It facilitates secure connectivity between public and private networks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.content.shi.com/SHIcom/ContentAttachmentImages/SharedResources/FBLP/Cisco/Cisco-091919-Simple-IT-Whitepaper.pdf

QUESTION 94 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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html

QUESTION 95 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 96 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 controllerC. management console and the cloud
D. SDN controller and the management solution

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97

```
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
```


Refer to the exhibit. 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 99 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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/security/ces/overview_guide/Cisco_Cloud_Hybrid_Email_Security_Overview_Guide.pdf

QUESTION 100 What is a characteristic of Cisco ASA Netflow v9 Secure Event Logging?

A. It tracks flow-create, flow-teardown, and flow-denied events.
B. It provides stateless IP flow tracking that exports all records of a specific flow.
C. It tracks the flow continuously and provides updates every 10 seconds.
D. Its events match all traffic classes in parallel.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/monitor-nsel.html

QUESTION 101 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 102 Which two kinds of attacks are prevented by multifactor authentication? (Choose two.)

A. phishing
B. brute force
C. man-in-the-middle
D. DDOS
E. tear drop

Correct Answer: BC

Section: (none)
Explanation

Explanation/Reference: