**QUESTION 57**
Which two capabilities does TAXII support? (Choose two.)

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

**Answer:** BC

**QUESTION 58**
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:**
https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-configguide-v622/platform_settings_policies_for_managed_devices.pdf

**QUESTION 59**
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

**Answer:** A
**Explanation:**

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 60**
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

**Answer:** AB
**Explanation:**
https://www.cisco.com/c/dam/en/us/products/collateral/security/cognitive-threat-analytics/at-aglance-c45-736555.pdf

**QUESTION 61**
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

**QUESTION 62**
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:**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnav/configuration/15-mt/sec-vpnavailability-15-mt-book/sec-state-fail-ipsec.html

**QUESTION 63**
What Cisco command shows you the status of an 802.1X connection on interface gi0/1?

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

**Answer:** B

**QUESTION 64**

A malicious user gained network access by spoofing printer connections that were authorized using MAB on four different switch ports at the same time.
What two catalyst switch security features will prevent further violations? (Choose two)

A. DHCP Snooping
B. 802.1AE MacSec
C. Port security
D. IP Device tracking
E. Dynamic ARP inspection
F. Private VLANs

**Answer:** AE

**QUESTION 65**
Which feature of Cisco ASA allows VPN users to be postured against Cisco ISE without requiring an inline posture node?

A. RADIUS Change of Authorization
B. device tracking
C. DHCP snooping
D. VLAN hopping

**Answer:** A

**QUESTION 66**
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:**
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-crc4.html#wp6039879000

**QUESTION 67**
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

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

**QUESTION 68**
Which solution protects hybrid cloud deployment workloads with application visibility and segmentation?

A. Nexus
B. Stealthwatch

C. Firepower
D. Tetration

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

**QUESTION 69**
What are the two most commonly used authentication factors in multifactor authentication? (Choose two.)

```
HQ_Router(config)# username admin5 privilege 5
HQ_Router(config)#privilege interface level 5 shutdown
HQ_Router(config)#privilege interface level 5 ip
HQ_Router(config)#privilege interface level 5 description
```

A. biometric factor
B. time factor
C. confidentiality factor
D. knowledge factor
E. encryption factor

**Answer:** AD

**QUESTION 70**
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:**
https://en.wikipediA.org/wiki/Advanced_Encryption_Standard

**QUESTION 71**
After deploying a Cisco ESA on your network, you notice that some messages fail to reach their destinations.
Which task can you perform to determine where each message was lost?

A. Configure the trackingconfig command to enable message tracking.
B. Generate a system report.
C. Review the log files.
D. Perform a trace.

**Answer:** A