

## RealTest.300-208 -244.Questions

Number: 300-208  
Passing Score: 800  
Time Limit: 120 min  
File Version: 24.05

**RealTest**

**300-208**

**IMPLEMENTING CISCO SECURE ACCESS  
SOLUTIONS**

- I only used these questions and got 480 marks with this. Perfect Show.
  - Added Explanations and Exhibits most of the questions.
- Many new questions are added , Good for review go ahead and pass the exam now.
  - Fixed the Exhibit size and Drag drops/hot spot questions.
  - Still valid , Hurry up guys study and pass this one.

## Exam A

### QUESTION 1

Which two Cisco Catalyst switch interface commands allow only a single voice device and a single data device to be connected to the IEEE 802.1X-enabled interface? (Choose two.)

- A. authentication host-mode single-host
- B. authentication host-mode multi-domain
- C. authentication host-mode multi-host
- D. authentication host-mode multi-auth

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 2

Which RADIUS attribute is used primarily to differentiate an IEEE 802.1x request from a Cisco MAB request?

- A. RADIUS Attribute (5) NAS-Port
- B. RADIUS Attribute (6) Service-Type
- C. RADIUS Attribute (7) Framed-Protocol
- D. RADIUS Attribute (61) NAS-Port-Type

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 3

Which authorization method is the Cisco best practice to allow endpoints access to the Apple App store or Google Play store with Cisco WLC software version 7.6 or newer?

- A. dACL
- B. DNS ACL
- C. DNS ACL defined in Cisco ISE

D. redirect ACL

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 4**

Which time allowance is the minimum that can be configured for posture reassessment interval?

- A. 5 minutes
- B. 20 minutes
- C. 60 minutes
- D. 90 minutes

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 5**

Which advanced authentication setting is needed to allow an unknown device to utilize Central WebAuth?

- A. If Authentication failed > Continue
- B. If Authentication failed > Drop
- C. If user not found > Continue
- D. If user not found > Reject

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is corrected.

#### **QUESTION 6**

Which option restricts guests from connecting more than one device at a time?

- A. Guest Portal policy > Set Device registration portal limit
- B. Guest Portal Policy > Set Allow only one guest session per user
- C. My Devices Portal > Set Maximum number of devices to register
- D. Multi-Portal Policy > Guest users should be able to do device registration

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 7**

In Cisco ISE, which two actions can be taken based on matching a profiler policy? (Choose two).

- A. exception
- B. network scan (NMAP)
- C. delete endpoint
- D. automatically remediate
- E. create matching identity group

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 8**

Which statement about the Cisco ISE BYOD feature is true?

- A. Use of SCEP/CA is optional.
- B. BYOD works only on wireless access.
- C. Cisco ISE needs to integrate with MDM to support BYOD.
- D. Only mobile endpoints are supported.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 9**

What user rights does an account need to join ISE to a Microsoft Active Directory domain?

- A. Create and Delete Computer Objects
- B. Domain Admin
- C. Join and Leave Domain
- D. Create and Delete User Objects

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 10**

A network administrator must enable which protocol to utilize EAP-Chaining?

- A. EAP-FAST
- B. EAP-TLS
- C. MSCHAPv2
- D. PEAP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 11**

The corporate security policy requires multiple elements to be matched in an authorization policy. Which elements can be combined to meet the requirement?

- A. Device registration status and device activation status
- B. Network access device and time condition

- C. User credentials and server certificate
- D. Built-in profile and custom profile

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 12**

In Cisco ISE, which probe must be enabled to collect profiling data using Device Sensor?

- A. RADIUS
- B. SNMPQuery
- C. SNMPTrap
- D. Network Scan
- E. Syslog

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 13**

Which two profile attributes can be collected by a Cisco Catalyst Switch that supports Device Sensor? (Choose two.)

- A. LLDP agent information
- B. user agent
- C. DHCP options
- D. open ports
- E. operating system
- F. trunk ports

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 14**

Which two profile attributes can be collected by a Cisco Wireless LAN Controller that supports Device Sensor? (Choose two.)

- A. LLDP agent information
- B. user agent
- C. DHCP options
- D. open ports
- E. CDP agent information
- F. FQDN

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 15**

Which statement about Cisco ISE BYOD is true?

- A. Dual SSID allows EAP-TLS only when connecting to the secured SSID.
- B. Single SSID does not require endpoints to be registered.
- C. Dual SSID allows BYOD for guest users.
- D. Single SSID utilizes open SSID to accommodate different types of users.
- E. Single SSID allows PEAP-MSCHAPv2 for native supplicant provisioning.

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 16**

Which two types of client provisioning resources are used for BYOD implementations? (Choose two.)

- A. user agent

- B. Cisco NAC agent
- C. native supplicant profiles
- D. device sensor
- E. software provisioning wizards

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 17**

Which protocol sends authentication and accounting in different requests?

- A. RADIUS
- B. TACACS+
- C. EAP-Chaining
- D. PEAP
- E. EAP-TLS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 18**

You enabled the guest session limit feature on the Cisco ISE. However, end users report that the same guest can log in from multiple devices simultaneously.

Which configuration is missing on the network access device?

- A. RADIUS authentication
- B. RADIUS accounting
- C. DHCP required
- D. AAA override

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**

corrected and modified.

**QUESTION 19**

A properly configured Cisco ISE Policy Service node is not receiving any profile data from a Cisco switch that runs Device Sensor.

Which option is the most likely reason for the failure?

- A. Syslog is configured for the Policy Administration Node.
- B. RADIUS Accounting is disabled.
- C. The SNMP community strings are mismatched.
- D. RADIUS Authentication is misconfigured.
- E. The connected endpoints support CDP but not DHCP.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

**Select and Place:**

Drag and drop the BYOD user experiences on an iPad on the left into the correct order on the right.

The CSR is generated on the endpoint and is sent to the Cisco ISE, which forwards it to the SCEP server

1

The user opens a web browser and is redirected to a registration portal

2

A CoA is issued and the endpoint is reconnected to the network with the proper access

3

The endpoint installs a signed certificate that is returned from the Cisco ISE along with the wireless network setting

4

The endpoint authenticates to secure SSID using the username and password

5

**Correct Answer:**

Drag and drop the BYOD user experiences on an iPad on the left into the correct order on the right.

	The endpoint authenticates to secure SSID using the username and password
	The user opens a web browser and is redirected to a registration portal
	The CSR is generated on the endpoint and is sent to the Cisco ISE, which forwards the CSR to the SCEP server
	The endpoint installs a signed certificate that is returned from the Cisco ISE along with the wireless network setting
	A CoA is issued and the endpoint is reconnected to the network with the proper access

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 21

A network administrator needs to implement a service that enables granular control of IOS commands that can be executed. Which AAA authentication method should be selected?

- A. TACACS+
- B. RADIUS
- C. Windows Active Directory
- D. Generic LDAP

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

An administrator can leverage which attribute to assign privileges based on Microsoft Active Directory user groups?

- A. member of
- B. group
- C. class
- D. person

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

Cisco 802.1X phasing enables flexible deployments through the use of open, low-impact, and closed modes. What is a unique characteristic of the most secure mode?

- A. Granular ACLs applied prior to authentication
- B. Per user dACLs applied after successful authentication
- C. Only EAPoL traffic allowed prior to authentication
- D. Adjustable 802.1X timers to enable successful authentication

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

A network administrator must enable which protocol extension to utilize EAP-Chaining?

- A. EAP-FAST
- B. EAP-TLS
- C. MSCHAPv2

D. PEAP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 25**

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 26**

Changes were made to the ISE server while troubleshooting, and now all wireless certificate authentications are failing. Logs indicate an EAP failure. What is the most likely cause of the problem?

- A. EAP-TLS is not checked in the Allowed Protocols list
- B. Certificate authentication profile is not configured in the Identity Store
- C. MS-CHAPv2 is not checked in the Allowed Protocols list
- D. Default rule denies all traffic
- E. Client root certificate is not included in the Certificate Store

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

The NAC Agent uses which port and protocol to send discovery packets to an ISE Policy Service Node?

- A. tcp/8905
- B. udp/8905
- C. http/80
- D. https/443

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 28**

Which two conditions are valid when configuring ISE for posturing? (Choose two.)

- A. Dictionary
- B. member Of
- C. Profile status
- D. File
- E. Service

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 29**

Refer to the exhibit.

```
device(config)#aaa new-model
device(config)#tacacs-server host 209.165.200.226
device(config)#tacacs-server host 209.165.200.227
device(config)#tacacs-server key 0 $$5@#$$!!1
```

Which three statements about the given configuration are true? (Choose three.)

- A. TACACS+ authentication configuration is complete.
- B. TACACS+ authentication configuration is incomplete.
- C. TACACS+ server hosts are configured correctly.
- D. TACACS+ server hosts are misconfigured.
- E. The TACACS+ server key is encrypted.
- F. The TACACS+ server key is unencrypted.

**Correct Answer:** BCF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 30

In AAA, what function does authentication perform?

- A. It identifies the actions that the user can perform on the device.
- B. It identifies the user who is trying to access a device.
- C. It identifies the actions that a user has previously taken.
- D. It identifies what the user can access.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 31

Which identity store option allows you to modify the directory services that run on TCP/IP?

- A. Lightweight Directory Access Protocol
- B. RSA SecurID server
- C. RADIUS
- D. Active Directory

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 32**

Which term describes a software application that seeks connectivity to the network via a network access device?

- A. authenticator
- B. server
- C. supplicant
- D. WLC

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33**

Cisco ISE distributed deployments support which three features? (Choose three.)

- A. global implementation of the profiler service CoA
- B. global implementation of the profiler service in Cisco ISE
- C. configuration to send system logs to the appropriate profiler node
- D. node-specific probe configuration
- E. server-specific probe configuration
- F. NetFlow probes

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

How frequently does the Profiled Endpoints dashlet refresh data?

- A. every 30 seconds
- B. every 60 seconds
- C. every 2 minutes
- D. every 5 minutes

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 35**

Which command in the My Devices Portal can restore a previously lost device to the network?

- A. Reset
- B. Found
- C. Reinstate
- D. Request

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 36**

What is the first step that occurs when provisioning a wired device in a BYOD scenario?

- A. The smart hub detects that the physically connected endpoint requires configuration and must use MAB to authenticate.
- B. The URL redirects to the Cisco ISE Guest Provisioning portal.
- C. Cisco ISE authenticates the user and deploys the SPW package.
- D. The device user attempts to access a network URL.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 37**

Which three features should be enabled as best practices for MAB? (Choose three.)

- A. MD5
- B. IP source guard
- C. DHCP snooping
- D. storm control
- E. DAI
- F. URPF

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 38**

When MAB is configured, how often are ports reauthenticated by default?

- A. every 60 seconds
- B. every 90 seconds
- C. every 120 seconds
- D. never

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 39**

What is a required step when you deploy dynamic VLAN and ACL assignments?

- A. Configure the VLAN assignment.

- B. Configure the ACL assignment.
- C. Configure Cisco IOS Software 802.1X authenticator authorization.
- D. Configure the Cisco IOS Software switch for ACL assignment.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 40**

Which model does Cisco support in a RADIUS change of authorization implementation?

- A. push
- B. pull
- C. policy
- D. security

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 41**

An organization has recently deployed ISE with the latest models of Cisco switches, and it plans to deploy Trustsec to secure its infrastructure. The company also wants to allow different network access policies for different user groups (e.g., administrators). Which solution is needed to achieve these goals?

- A. Cisco Security Group Access Policies in order to use SGACLs to control access based on SGTs assigned to different users
- B. MACsec in Multiple-Host Mode in order to open or close a port based on a single authentication
- C. Identity-based ACLs on the switches with user identities provided by ISE
- D. Cisco Threat Defense for user group control by leveraging Netflow exported from the switches and login information from ISE

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 42**

Security Group Access requires which three syslog messages to be sent to Cisco ISE? (Choose three.)

- A. IOS-7-PROXY\_DROP
- B. AP-1-AUTH\_PROXY\_DOS\_ATTACK
- C. MKA-2-MACDROP
- D. AUTHMGR-5-MACMOVE
- E. ASA-6-CONNECT\_BUILT
- F. AP-1-AUTH\_PROXY\_FALLBACK\_REQ

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

Which administrative role has permission to assign Security Group Access Control Lists?

- A. System Admin
- B. Network Device Admin
- C. Policy Admin
- D. Identity Admin

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

Refer to the exhibit.

```
asal(config)# time-range WeekendHours
asal(config-time-range)# periodic friday 18:00 to monday 8:00
asal(config)# access-list Outside extended deny ip any object-group vpnserver time-range WeekendHours log
asal(config)# access-group Outside in outside
```

If the given configuration is applied to the object-group vpnserver, during which time period are external users able to connect?

- A. From Friday at 6:00 p.m. until Monday at 8:00 a.m.
- B. From Monday at 8:00 a.m. until Friday at 6:00 p.m.
- C. From Friday at 6:01 p.m. until Monday at 8:01 a.m.
- D. From Monday at 8:01 a.m. until Friday at 5:59 p.m.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 45

Which set of commands allows IPX inbound on all interfaces?

- A. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow in interface global
- B. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow in interface inside
- C. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow in interface outside
- D. ASA1(config)# access-list IPX-Allow ethertype permit ipx ASA1(config)# access-group IPX-Allow out interface global

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

modified.

#### QUESTION 46

Which command enables static PAT for TCP port 25?

- A. nat (outside,inside) static 209.165.201.3 209.165.201.226 eq smtp

- B. nat static 209.165.201.3 eq smtp
- C. nat (inside,outside) static 209.165.201.3 service tcp smtp smtp
- D. static (inside,outside) 209.165.201.3 209.165.201.226 netmask 255.255.255.255

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 47**

Which command is useful when troubleshooting AAA Authentication between a Cisco router and the AAA server?

- A. test aaa-server test cisco cisco123 all new-code
- B. test aaa group7 tacacs+ auth cisco123 new-code
- C. test aaa group tacacs+ cisco cisco123 new-code
- D. test aaa-server tacacs+ group7 cisco cisco123 new-code

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 48**

In a multi-node ISE deployment, backups are not working on the MnT node. Which ISE CLI option would help mitigate this issue?

- A. repository
- B. ftp-url
- C. application-bundle
- D. collector

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

Which command can check a AAA server authentication for server group Group1, user cisco, and password cisco555 on a Cisco ASA device?

- A. ASA# test aaa-server authentication Group1 username cisco password cisco555
- B. ASA# test aaa-server authentication group Group1 username cisco password cisco555
- C. ASA# aaa-server authorization Group1 username cisco password cisco555
- D. ASA# aaa-server authentication Group1 roger cisco555

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

Which statement about system time and NTP server configuration with Cisco ISE is true?

- A. The system time and NTP server settings can be configured centrally on the Cisco ISE.
- B. The system time can be configured centrally on the Cisco ISE, but NTP server settings must be configured individually on each ISE node.
- C. NTP server settings can be configured centrally on the Cisco ISE, but the system time must be configured individually on each ISE node.
- D. The system time and NTP server settings must be configured individually on each ISE node.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 51**

Which two are characteristics of GETVPN? (Choose two.)

- A. The IP header of the encrypted packet is preserved
- B. A key server is elected among all configured Group Members
- C. Unique encryption keys are computed for each Group Member
- D. The same key encryption and traffic encryption keys are distributed to all Group Members

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 52**

A company has decided to migrate an existing IKEv1 VPN tunnel to IKEv2. Which two are valid configuration constructs on a Cisco IOS router? (Choose two.)

- A. `crypto ikev2 keyring keyring-name`  
`peer peer1`  
`address 209.165.201.1 255.255.255.255`  
`pre-shared-key local key1`  
`pre-shared-key remote key2`
- B. `crypto ikev2 transform-set transform-set-name`  
`esp-3des esp-md5-hmac`  
`esp-aes esp-sha-hmac`
- C. `crypto ikev2 map crypto-map-name`  
`set crypto ikev2 tunnel-group tunnel-group-name`  
`set crypto ikev2 transform-set transform-set-name`
- D. `crypto ikev2 tunnel-group tunnel-group-name`  
`match identity remote address 209.165.201.1`  
`authentication local pre-share`  
`authentication remote pre-share`
- E. `crypto ikev2 profile profile-name`  
`match identity remote address 209.165.201.1`  
`authentication local pre-share`  
`authentication remote pre-share`

**Correct Answer: AE**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 53**

Which four activities does the Key Server perform in a GETVPN deployment? (Choose four.)

- A. authenticates group members
- B. manages security policy

- C. creates group keys
- D. distributes policy/keys
- E. encrypts endpoint traffic
- F. receives policy/keys
- G. defines group members

**Correct Answer:** ABCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 54**

Where is split-tunneling defined for remote access clients on an ASA?

- A. Group-policy
- B. Tunnel-group
- C. Crypto-map
- D. Web-VPN Portal
- E. ISAKMP client

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 55**

Which of the following could be used to configure remote access VPN Host-scan and pre-login policies?

- A. ASDM
- B. Connection-profile CLI command
- C. Host-scan CLI command under the VPN group policy
- D. Pre-login-check CLI command

**Correct Answer:** A

**Section:** (none)

### Explanation

#### Explanation/Reference:

valid and updated.

#### QUESTION 56

In FlexVPN, what command can an administrator use to create a virtual template interface that can be configured and applied dynamically to create virtual access interfaces?

- A. interface virtual-template number type template
- B. interface virtual-template number type tunnel
- C. interface template number type virtual
- D. interface tunnel-template number

**Correct Answer:** B

**Section:** (none)

#### Explanation

#### Explanation/Reference:

Hello - here is a reference an explanation that can be included with this test.

[http://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_conn\\_ike2vpn/configuration/15-2mt/sec-flex-spoke.html#GUID-4A10927D-4C6A-4202-B01C-DA7E462F5D8A](http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-flex-spoke.html#GUID-4A10927D-4C6A-4202-B01C-DA7E462F5D8A)

Configuring the Virtual Tunnel Interface on FlexVPN Spoke

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface virtual-template number type tunnel
4. ip unnumbered tunnel number
5. ip nhrp network-id number
6. ip nhrp shortcut virtual-template-number
7. ip nhrp redirect [timeout seconds]
8. exit

#### QUESTION 57

In FlexVPN, what is the role of a NHRP resolution request?

- A. It allows these entities to directly communicate without requiring traffic to use an intermediate hop
- B. It dynamically assigns VPN users to a group
- C. It blocks these entities from to directly communicating with each other

D. It makes sure that each VPN spoke directly communicates with the hub

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 58**

What are three benefits of deploying a GET VPN? (Choose three.)

- A. It provides highly scalable point-to-point topologies.
- B. It allows replication of packets after encryption.
- C. It is suited for enterprises running over a DMVPN network.
- D. It preserves original source and destination IP address information.
- E. It simplifies encryption management through use of group keying.
- F. It supports non-IP protocols.

**Correct Answer:** BDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 59**

What is the default topology type for a GET VPN?

- A. point-to-point
- B. hub-and-spoke
- C. full mesh
- D. on-demand spoke-to-spoke

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

Which two GDOI encryption keys are used within a GET VPN network? (Choose two.)

- A. key encryption key
- B. group encryption key
- C. user encryption key
- D. traffic encryption key

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 61**

What are the three primary components of a GET VPN network? (Choose three.)

- A. Group Domain of Interpretation protocol
- B. Simple Network Management Protocol
- C. server load balancer
- D. accounting server
- E. group member
- F. key server

**Correct Answer:** AEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

Which two IKEv1 policy options must match on each peer when you configure an IPsec site-to-site VPN? (Choose two.)

- A. priority number
- B. hash algorithm
- C. encryption algorithm
- D. session lifetime

E. PRF algorithm

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 63**

Which two parameters are configured within an IKEv2 proposal on an IOS router? (Choose two.)

- A. authentication
- B. encryption
- C. integrity
- D. lifetime

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 64**

In a spoke-to-spoke DMVPN topology, which type of interface does a branch router require?

- A. Virtual tunnel interface
- B. Multipoint GRE interface
- C. Point-to-point GRE interface
- D. Loopback interface

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 65**

Refer to the exhibit.

```
crypto pki certificate map CERTMAP
subject-name co cn=cisco.com
crypto ikev2 profile IKEPROFILE
authentication local pre-share
authentication remote rsa-sig
keyring local KEYRING1
match identity remote address 209.165.200.225 255.255.255.255
match identity remote address 209.165.202.155 255.255.255.255
match certificate CERTMAP
pki trustpoint TRUSTPOINT1
```

After the configuration is performed, which combination of devices can connect?

- A. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name of "cisco.com"
- B. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 or a certificate with subject name containing "cisco.com"
- C. a device with an identity type of IPv4 address of both 209.165.200.225 and 209.165.202.155 and a certificate with subject name containing "cisco.com"
- D. a device with an identity type of IPv4 address of 209.165.200.225 or 209.165.202.155 or a certificate with subject name containing "cisco.com"

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 66

Which three settings are required for crypto map configuration? (Choose three.)

- A. match address
- B. set peer
- C. set transform-set
- D. set security-association lifetime
- E. set security-association level per-host
- F. set pfs

**Correct Answer:** ABC

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 67**

A network is configured to allow clientless access to resources inside the network. Which feature must be enabled and configured to allow SSH applications to respond on the specified port 8889?

- A. auto applet download
- B. port forwarding
- C. web-type ACL
- D. HTTP proxy

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 68**

Consider this scenario. When users attempt to connect via a Cisco AnyConnect VPN session, the certificate has changed and the connection fails.

What is a possible cause of the connection failure?

- A. An invalid modulus was used to generate the initial key.
- B. The VPN is using an expired certificate.
- C. The Cisco ASA appliance was reloaded.
- D. The Trusted Root Store is configured incorrectly.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 69**

In the Cisco ASDM interface, where do you enable the DTLS protocol setting?

- A. Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy
- B. Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit
- C. Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- D. Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The reference:

[http://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect20/administrative/guide/admin/admin5.html](http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/admin/admin5.html)

Shows where DTLS can be configured as:

- Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit > Add or Edit Internal Group Policy > Advanced > SSL VPN Client
- Configuration > Remote Access VPN > Network (Client) Access > AAA Setup > Local Users > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client
- Device Management > Users/AAA > User Accounts > Add or Edit > Add or Edit User Account > VPN Policy > SSL VPN Client

#### **QUESTION 70**

What are two forms of SSL VPN? (Choose two.)

- A. port forwarding
- B. Full Tunnel Mode
- C. Cisco IOS WebVPN
- D. Cisco AnyConnect

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 71**

When Cisco ASA applies VPN permissions, what is the first set of attributes that it applies?

- A. dynamic access policy attributes
- B. group policy attributes
- C. connection profile attributes
- D. user attributes

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 72**

What are two variables for configuring clientless SSL VPN single sign-on? (Choose two.)

- A. CSCO\_WEBVPN\_OTP\_PASSWORD
- B. CSCO\_WEBVPN\_INTERNAL\_PASSWORD
- C. CSCO\_WEBVPN\_USERNAME
- D. CSCO\_WEBVPN\_RADIUS\_USER

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 73**

To change the title panel on the logon page of the Cisco IOS WebVPN portal, which file must you configure?

- A. Cisco IOS WebVPN customization template
- B. Cisco IOS WebVPN customization general
- C. web-access-hlp.inc
- D. app-access-hlp.inc

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 74**

Which three plugins are available for clientless SSL VPN? (Choose three.)

- A. CIFS
- B. RDP2
- C. SSH
- D. VNC
- E. SQLNET
- F. ICMP

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 75**

Which command simplifies the task of converting an SSL VPN to an IKEv2 VPN on a Cisco ASA appliance that has an invalid IKEv2 configuration?

- A. migrate remote-access ssl overwrite
- B. migrate remote-access ikev2
- C. migrate l2l
- D. migrate remote-access ssl

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Below is a reference for this question:

<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113597-ptn-113597.html>

If your IKEv1, or even SSL, configuration already exists, the ASA makes the migration process simple. On the command line, enter the migrate command:

migrate {l2l | remote-access {ikev2 | ssl} | overwrite} Things of note:

Keyword definitions:

I2I - This converts current IKEv1 I2I tunnels to IKEv2.

remote access - This converts the remote access configuration. You can convert either the IKEv1 or the SSL tunnel groups to IKEv2.

overwrite - If you have a IKEv2 configuration that you wish to overwrite, then this keyword converts the current IKEv1 configuration and removes the superfluous IKEv2 configuration.

#### **QUESTION 76**

Which statement describes a prerequisite for single-sign-on Netegrity Cookie Support in an IOC SSL VPN?

- A. The Cisco AnyConnect Secure Mobility Client must be installed in flash.
- B. A SiteMinder plug-in must be installed on the Cisco SSL VPN gateway.
- C. A Cisco plug-in must be installed on a SiteMinder server.
- D. The Cisco Secure Desktop software package must be installed in flash.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 77**

Which two statements describe effects of the DoNothing option within the untrusted network policy on a Cisco AnyConnect profile? (Choose two.)

- A. The client initiates a VPN connection upon detection of an untrusted network.
- B. The client initiates a VPN connection upon detection of a trusted network.
- C. The always-on feature is enabled.
- D. The always-on feature is disabled.
- E. The client does not automatically initiate any VPN connection.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 78**

Which command enables IOS SSL VPN Smart Tunnel support for PuTTY?

- A. appl ssh putty.exe win
- B. appl ssh putty.exe windows
- C. appl ssh putty
- D. appl ssh putty.exe

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 79**

Which three remote access VPN methods in an ASA appliance provide support for Cisco Secure Desktop? (Choose three.)

- A. IKEv1
- B. IKEv2
- C. SSL client
- D. SSL clientless
- E. ESP
- F. L2TP

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 80**

A user is unable to establish an AnyConnect VPN connection to an ASA. When using the Real- Time Log viewer within ASDM to troubleshoot the issue, which two filter options would the administrator choose to show only syslog messages relevant to the VPN connection? (Choose two.)

- A. Client's public IP address
- B. Client's operating system
- C. Client's default gateway IP address
- D. Client's username
- E. ASA's public IP address

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 81**

Which Cisco ASDM option configures forwarding syslog messages to email?

- A. Configuration > Device Management > Logging > E-Mail Setup
- B. Configuration > Device Management > E-Mail Setup > Logging Enable
- C. Select the syslogs to email, click Edit, and select the Forward Messages option.
- D. Select the syslogs to email, click Settings, and specify the Destination Email Address option.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 82**

Which three network access devices allow for static security group tag assignment? (Choose three.)

- A. intrusion prevention system
- B. access layer switch
- C. data center access switch
- D. load balancer
- E. VPN concentrator
- F. wireless LAN controller

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 83**

Which option is required for inline security group tag propagation?

- A. Cisco Secure Access Control System
- B. hardware support
- C. Security Group Tag Exchange Protocol (SXP) v4
- D. Cisco Identity Services Engine

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 84**

Which two fields are characteristics of IEEE 802.1AE frame? (Choose two.)

- A. destination MAC address
- B. source MAC address
- C. 802.1AE header in EtherType
- D. security group tag in EtherType
- E. integrity check value
- F. CRC/FCS

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 85**

Which two options are valid for configuring IEEE 802.1AE MACSec between switches in a TrustSec network? (Choose two.)

- A. manually on links between supported switches
- B. in the Cisco Identity Services Engine
- C. in the global configuration of a TrustSec non-seed switch
- D. dynamically on links between supported switches

- E. in the Cisco Secure Access Control System
- F. in the global configuration of a TrustSec seed switch

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 86**

Wireless client supplicants attempting to authenticate to a wireless network are generating excessive log messages. Which three WLC authentication settings should be disabled? (Choose three.)

- A. RADIUS Server Timeout
- B. RADIUS Aggressive-Failover
- C. Idle Timer
- D. Session Timeout
- E. Client Exclusion
- F. Roaming

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 87**

Which two authentication stores are supported to design a wireless network using PEAP EAP- MSCHAPv2 as the authentication method? (Choose two.)

- A. Microsoft Active Directory
- B. ACS
- C. LDAP
- D. RSA Secure-ID
- E. Certificate Server

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88**

What is another term for 802.11i wireless network security?

- A. 802.1x
- B. WEP
- C. TKIP
- D. WPA
- E. WPA2

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 89**

Which two EAP types require server side certificates? (Choose two.)

- A. EAP-TLS
- B. PEAP
- C. EAP-MD5
- D. LEAP
- E. EAP-FAST
- F. MSCHAPv2

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 90**

Where is client traffic decrypted in a controller-based wireless network protected with WPA2 Security?

- A. Access Point
- B. Switch
- C. Wireless LAN Controller
- D. Authentication Server

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 91**

Wireless client supplicants attempting to authenticate to a wireless network are generating excessive log messages. Which three WLC authentication settings should be disabled? (Choose three.)

- A. RADIUS Server Timeout
- B. RADIUS Aggressive-Failover
- C. Idle Timer
- D. Session Timeout
- E. Client Exclusion
- F. Roaming

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 92**

Which two authentication stores are supported to design a wireless network using PEAP EAP- MSCHAPv2 as the authentication method? (Choose two.)

- A. Microsoft Active Directory
- B. ACS
- C. LDAP
- D. RSA Secure-ID
- E. Certificate Server

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 93**

What is another term for 802.11i wireless network security?

- A. 802.1x
- B. WEP
- C. TKIP
- D. WPA
- E. WPA2

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 94**

Which two EAP types require server side certificates? (Choose two.)

- A. EAP-TLS
- B. PEAP
- C. EAP-MD5
- D. LEAP
- E. EAP-FAST
- F. MSCHAPv2

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

Where is client traffic decrypted in a controller-based wireless network protected with WPA2 Security?

- A. Access Point
- B. Switch
- C. Wireless LAN Controller
- D. Authentication Server

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 96**

Which setting provides the best security for a WLAN and authenticates users against a centralized directory store?

- A. WPA2 AES-CCMP and 801.X authentication
- B. WPA2 AES-CCMP and PSK authentication
- C. WPA2 TKIP and PSK authentication
- D. WPA2 TKIP and 802.1X authentication

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 97**

What is a feature of Cisco WLC and IPS synchronization?

- A. Cisco WLC populates the ACLs to prevent repeat intruder attacks.
- B. The IPS automatically send shuns to Cisco WLC for an active host block.
- C. Cisco WLC and IPS synchronization enables faster wireless access.
- D. IPS synchronization uses network access points to provide reliable monitoring.

**Correct Answer:** B

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 98

Which two components are required to connect to a WLAN network that is secured by EAP-TLS authentication? (Choose two.)

- A. Kerberos authentication server
- B. AAA/RADIUS server
- C. PSKs
- D. CA server

**Correct Answer:** BD

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 99

Which statement about Cisco Management Frame Protection is true?

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.

**Correct Answer:** D

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 100

Which three statements about the Cisco wireless IPS solution are true? (Choose three.)

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.

- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.
- E. It allows the WLC to failover because of congestion.

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 101**

In a basic ACS deployment consisting of two servers, for which three tasks is the primary server responsible? (Choose three.)

- A. configuration
- B. authentication
- C. sensing
- D. policy requirements
- E. monitoring
- F. repudiation

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 102**

What are the initial steps must you perform to add the ISE to the WLC?

- A. 1. With a Web browser, establish an HTTP connection to the WLC pod.  
2. Navigate to Administration > Authentication > New.  
3. Enter server values to begin the configuration.
- B. 1. With a Web browser, establish an FTP connection to the WLC pod.  
2. Navigate to Security > Administration > New.  
3. Add additional security features for FTP authentication.
- C. 1. With a Web browser, establish an HTTP connection to the WLC pod.  
2. Navigate to Authentication > New.  
3. Enter ACLs and Authentication methods to begin the configuration.

- D. 1. With a Web browser connect, establish an HTTPS connection to the WLC pod.  
2. Navigate to Security > Authentication > New.  
3. Enter server values to begin the configuration.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 103

Which command configures console port authorization under line con 0?

- A. authorization default|WORD
- B. authorization exec line con 0|WORD
- C. authorization line con 0|WORD
- D. authorization exec default|WORD

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 104

Which two statements about administrative access to the ACS Solution Engine are true? (Choose two.)

- A. The ACS Solution Engine supports command-line connections through a serial-port connection.
- B. For GUI access, an administrative GUI user must be created with the add-guiadmin command.
- C. The ACS Solution Engine supports command-line connections through an Ethernet interface.
- D. An ACL-based policy must be configured to allow administrative-user access.
- E. GUI access to the ACS Solution Engine is not supported.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 105**

What is the purpose of the Cisco ISE Guest Service Sponsor Portal?

- A. It tracks and stores user activity while connected to the Cisco ISE.
- B. It securely authenticates guest users for the Cisco ISE Guest Service.
- C. It filters guest users from account holders to the Cisco ISE.
- D. It creates and manages Guest User accounts.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 106**

What is the effect of the ip http secure-server command on a Cisco ISE?

- A. It enables the HTTP server for users to connect on the command line.
- B. It enables the HTTP server for users to connect using Web-based authentication.
- C. It enables the HTTPS server for users to connect using Web-based authentication.
- D. It enables the HTTPS server for users to connect on the command line.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 107**

When RADIUS NAC and AAA Override are enabled for WLC on a Cisco ISE, which two statements about RADIUS NAC are true? (Choose two.)

- A. It will return an access-accept and send the redirection URL for all users.
- B. It establishes secure connectivity between the RADIUS server and the ISE.
- C. It allows the ISE to send a CoA request that indicates when the user is authenticated.
- D. It is used for posture assessment, so the ISE changes the user profile based on posture result.
- E. It allows multiple users to authenticate at the same time.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 108**

What are the initial steps to configure an ACS as a TACACS server?

- A. 1. Choose Network Devices and AAA Clients > Network Resources.  
2. Click Create.
- B. 1. Choose Network Resources > Network Devices and AAA Clients.  
2. Click Create.
- C. 1. Choose Network Resources > Network Devices and AAA Clients.  
2. Click Manage.
- D. 1. Choose Network Devices and AAA Clients > Network Resources.  
2. Click Install.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 109**

Which two statements about administrative access to the Cisco Secure ACS SE are true? (Choose two.)

- A. The Cisco Secure ACS SE supports command-line connections through a serial-port connection.
- B. For GUI access, an administrative GUI user must be created by using the add-guiadmin command.
- C. The Cisco Secure ACS SE supports command-line connections through an Ethernet interface.
- D. An ACL-based policy must be configured to allow administrative-user access.
- E. GUI access to the Cisco Secure ASC SE is not supported.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 110**

When RADIUS NAC and AAA Override are enabled for a WLC on a Cisco ISE, which two statements about RADIUS NAC are true? (Choose two.)

- A. It returns an access-accept and sends the redirection URL for all users.
- B. It establishes secure connectivity between the RADIUS server and the Cisco ISE.
- C. It allows the Cisco ISE to send a CoA request that indicates when the user is authenticated.
- D. It is used for posture assessment, so the Cisco ISE changes the user profile based on posture result.
- E. It allows multiple users to authenticate at the same time.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 111**

Which three are required steps to enable SXP on a Cisco ASA? (Choose three).

- A. configure AAA authentication
- B. configure password
- C. issue the aaa authorization command aaa-server group command
- D. configure a peer
- E. configure TACACS
- F. issue the cts sxp enable command

**Correct Answer:** BDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 112**

Which three network access devices allow for static security group tag assignment? (Choose three.)

- A. intrusion prevention system
- B. access layer switch

- C. data center access switch
- D. load balancer
- E. VPN concentrator
- F. wireless LAN controller

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is valid.

### **QUESTION 113**

Which option is required for inline security group tag propagation?

- A. Cisco Secure Access Control System
- B. hardware support
- C. Security Group Tag Exchange Protocol (SXP) v4
- D. Cisco Identity Services Engine

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### **QUESTION 114**

Which two fields are characteristics of IEEE 802.1AE frame? (Choose two.)

- A. destination MAC address
- B. source MAC address
- C. 802.1AE header in EtherType
- D. security group tag in EtherType
- E. integrity check value
- F. CRC/FCS

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 115**

Which two options are valid for configuring IEEE 802.1AE MACSec between switches in a TrustSec network? (Choose two.)

- A. manually on links between supported switches
- B. in the Cisco Identity Services Engine
- C. in the global configuration of a TrustSec non-seed switch
- D. dynamically on links between supported switches
- E. in the Cisco Secure Access Control System
- F. in the global configuration of a TrustSec seed switch

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 116**

Which three pieces of information can be found in an authentication detail report? (Choose three.)

- A. DHCP vendor ID
- B. user agent string
- C. the authorization rule matched by the endpoint
- D. the EAP method the endpoint is using
- E. the RADIUS username being used
- F. failed posture requirement

**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 117**

Certain endpoints are missing DHCP profiling data.

Which option describes what can be used to determine if DHCP requests from clients are reaching Cisco ISE?

- A. output of show interface gigabitEthernet 0 from the CLI
- B. output of debug logging all 7 from the CLI
- C. output of show logging application profiler.log from the CLI
- D. the TCP dump diagnostic tool through the GUI
- E. the posture troubleshooting diagnostic tool through the GUI

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 118**

Which debug command on a Cisco WLC shows the reason that a client session was terminated?

- A. debug dot11 state enable
- B. debug dot1x packet enable
- C. debug client mac addr
- D. debug dtls event enable
- E. debug ap enable cisco ap

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 119**

Which two identity databases are supported when PEAP-MSCHAPv2 is used as EAP type? (Choose two.)

- A. Windows Active Directory
- B. LDAP
- C. RADIUS token server
- D. internal endpoint store

- E. internal user store
- F. certificate authentication profile
- G. RSA SecurID

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 120**

Which two Cisco Catalyst switch interface commands allow only a single voice device and a single data device to be connected to the IEEE 802.1X-enabled interface? (Choose two.)

- A. authentication host-mode single-host
- B. authentication host-mode multi-domain
- C. authentication host-mode multi-host
- D. authentication host-mode multi-auth

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 121**

Which RADIUS attribute is used primarily to differentiate an IEEE 802.1x request from a Cisco MAB request?

- A. RADIUS Attribute (5) NAS-Port
- B. RADIUS Attribute (6) Service-Type
- C. RADIUS Attribute (7) Framed-Protocol
- D. RADIUS Attribute (61) NAS-Port-Type

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 122**

Which authorization method is the Cisco best practice to allow endpoints access to the Apple App store or Google Play store with Cisco WLC software version 7.6 or newer?

- A. dACL
- B. DNS ACL
- C. DNS ACL defined in Cisco ISE
- D. redirect ACL

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 123**

Which time allowance is the minimum that can be configured for posture reassessment interval?

- A. 5 minutes
- B. 20 minutes
- C. 60 minutes
- D. 90 minutes

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 124**

Which advanced authentication setting is needed to allow an unknown device to utilize Central WebAuth?

- A. If Authentication failed > Continue
- B. If Authentication failed > Drop
- C. If user not found > Continue
- D. If user not found > Reject

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 125**

Which option restricts guests from connecting more than one device at a time?

- A. Guest Portal policy > Set Device registration portal limit
- B. Guest Portal Policy > Set Allow only one guest session per user
- C. My Devices Portal > Set Maximum number of devices to register
- D. Multi-Portal Policy > Guest users should be able to do device registration

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 126**

In Cisco ISE, which two actions can be taken based on matching a profiler policy? (Choose two).

- A. exception
- B. network scan (NMAP)
- C. delete endpoint
- D. automatically remediate
- E. create matching identity group

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 127**

Which statement about the Cisco ISE BYOD feature is true?

- A. Use of SCEP/CA is optional.
- B. BYOD works only on wireless access.
- C. Cisco ISE needs to integrate with MDM to support BYOD.
- D. Only mobile endpoints are supported.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 128**

What user rights does an account need to join ISE to a Microsoft Active Directory domain?

- A. Create and Delete Computer Objects
- B. Domain Admin
- C. Join and Leave Domain
- D. Create and Delete User Objects

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 129**

A network administrator must enable which protocol to utilize EAP-Chaining?

- A. EAP-FAST
- B. EAP-TLS
- C. MSCHAPv2
- D. PEAP

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 130**

The corporate security policy requires multiple elements to be matched in an authorization policy. Which elements can be combined to meet the requirement?

- A. Device registration status and device activation status
- B. Network access device and time condition
- C. User credentials and server certificate
- D. Built-in profile and custom profile

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 131**

A network administrator needs to determine the ability of existing network devices to deliver key BYOD services. Which tool will complete a readiness assessment and outline hardware and software capable and incapable devices?

- A. Prime Infrastructure
- B. Network Control System
- C. Cisco Security Manager
- D. Identity Services Engine

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

corrected and modified.

**QUESTION 132**

Which EAP method uses a modified version of the MS-CHAP authentication protocol?

- A. EAP-POTP
- B. EAP-TLS

- C. LEAP
- D. EAP-MD5

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 133**

Under which circumstance would an inline posture node be deployed?

- A. When the NAD does not support CoA
- B. When the NAD cannot support the number of connected endpoints
- C. When a PSN is overloaded
- D. To provide redundancy for a PSN

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 134**

Which Cisco ISE 1.x protocol can be used to control admin access to network access devices?

- A. TACACS+
- B. RADIUS
- C. EAP
- D. Kerberos

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 135**

A user is on a wired connection and the posture status is noncompliant.

Which state will their EPS session be placed in?

- A. disconnected
- B. limited
- C. no access
- D. quarantined

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 136**

Which three posture states can be used for authorization rules? (Choose three.)

- A. unknown
- B. known
- C. noncompliant
- D. quarantined
- E. compliant
- F. no access
- G. limited

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 137**

Which two Cisco ISE administration options are available in the Default Posture Status setting? (Choose two.)

- A. Unknown
- B. Compliant

- C. FailOpen
- D. FailClose
- E. Noncompliant

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 138**

Which two portals can be configured to use portal FQDN? (Choose two.)

- A. admin
- B. sponsor
- C. guest
- D. my devices
- E. monitoring and troubleshooting

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 139**

Which five portals are provided by PSN? (Choose five.)

- A. guest
- B. sponsor
- C. my devices
- D. blacklist
- E. client provisioning
- F. admin
- G. monitoring and troubleshooting

**Correct Answer:** ABCDE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Answer: A, B, C, D, E

**QUESTION 140**

When you add a new PSN for guest access services, which two options must be enabled under deployment settings? (Choose two.)

- A. Admin
- B. Monitoring
- C. Policy Service
- D. Session Services
- E. Profiling

**Correct Answer: CD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 141**

Which two features are required when configuring a DMVPN network? (Choose two.)

- A. Dynamic routing protocol
- B. GRE tunnel interface
- C. Next Hop Resolution Protocol
- D. Dynamic crypto map
- E. IPsec encryption

**Correct Answer: BC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 142**

What are two benefits of DMVPN Phase 3? (Choose two.)

- A. Administrators can use summarization of routing protocol updates from hub to spokes.
- B. It introduces hierarchical DMVPN deployments.
- C. It introduces non-hierarchical DMVPN deployments.
- D. It supports L2TP over IPsec as one of the VPN protocols.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 143**

Which are two main use cases for Clientless SSL VPN? (Choose two.)

- A. In kiosks that are part of a shared environment
- B. When the users do not have admin rights to install a new VPN client
- C. When full tunneling is needed to support applications that use TCP, UDP, and ICMP
- D. To create VPN site-to-site tunnels in combination with remote access

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 144**

Which technology can rate-limit the number of tunnels on a DMVPN hub when system utilization is above a specified percentage?

- A. NHRP Event Publisher
- B. interface state control
- C. CAC
- D. NHRP Authentication
- E. ip nhrp connect

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 145**

Which technology supports tunnel interfaces while remaining compatible with legacy VPN implementations?

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

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 146**

Which IKEv2 feature minimizes the configuration of a FlexVPN on Cisco IOS devices?

- A. IKEv2 Suite-B
- B. IKEv2 proposals
- C. IKEv2 profiles
- D. IKEv2 Smart Defaults

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 147**

When an IPsec SVTI is configured, which technology processes traffic forwarding for encryption?

- A. ACL
- B. IP routing
- C. RRI

D. front door VPN routing and forwarding

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 148**

An IOS SSL VPN is configured to forward TCP ports. A remote user cannot access the corporate FTP site with a Web browser. What is a possible reason for the failure?

- A. The user's FTP application is not supported.
- B. The user is connecting to an IOS VPN gateway configured in Thin Client Mode.
- C. The user is connecting to an IOS VPN gateway configured in Tunnel Mode.
- D. The user's operating system is not supported.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

<http://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70664-IOSthinclient.html> Thin-Client SSL VPN (Port Forwarding)

A remote client must download a small, Java-based applet for secure access of TCP applications that use static port numbers. UDP is not supported. Examples include access to POP3, SMTP, IMAP, SSH, and Telnet. The user needs local administrative privileges because changes are made to files on the local machine. This method of SSL VPN does not work with applications that use dynamic port assignments, for example, several FTP applications.

#### **QUESTION 149**

A Cisco IOS SSL VPN gateway is configured to operate in clientless mode so that users can access file shares on a Microsoft Windows 2003 server. Which protocol is used between the Cisco IOS router and the Windows server?

- A. HTTPS
- B. NetBIOS
- C. CIFS
- D. HTTP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 150**

The NAC Agent v4.9.x uses which ports and protocols to communicate with an ISE Policy Service Node?

- A. tcp/8905, http/80, ftp/21
- B. tcp/8905, http/80, https/443
- C. udp/8905, telnet/23, https/443
- D. udp/8906, http/80, https/443

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 151**

Which setting provides the best security for a WLAN and authenticates users against a centralized directory store?

- A. WPA2 AES-CCMP and 801.X authentication
- B. WPA2 AES-CCMP and PSK authentication
- C. WPA2 TKIP and PSK authentication
- D. WPA2 TKIP and 802.1X authentication

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

answer is well defined.

**QUESTION 152**

What is a feature of Cisco WLC and IPS synchronization?

- A. Cisco WLC populates the ACLs to prevent repeat intruder attacks.
- B. The IPS automatically send shuns to Cisco WLC for an active host block.

- C. Cisco WLC and IPS synchronization enables faster wireless access.
- D. IPS synchronization uses network access points to provide reliable monitoring.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 153**

Which two components are required to connect to a WLAN network that is secured by EAP-TLS authentication? (Choose two.)

- A. Kerberos authentication server
- B. AAA/RADIUS server
- C. PSKs
- D. CA server

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 154**

Which statement about Cisco Management Frame Protection is true?

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 155**

Which three statements about the Cisco wireless IPS solution are true? (Choose three.)

- A. It enables stations to remain in power-save mode, except at specified intervals to receive data from the access point.
- B. It detects spoofed MAC addresses.
- C. It identifies potential RF jamming attacks.
- D. It protects against frame and device spoofing.
- E. It allows the WLC to failover because of congestion.

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 156**

In a basic ACS deployment consisting of two servers, for which three tasks is the primary server responsible? (Choose three.)

- A. configuration
- B. authentication
- C. sensing
- D. policy requirements
- E. monitoring
- F. repudiation

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 157**

In a split ACS deployment with primary and secondary servers, which three statements about AAA load handling are true? (Choose three.)

- A. During normal operations, each server processes the full workload of both servers.
- B. If a AAA connectivity problem occurs, the servers split the full load of authentication requests.
- C. If a AAA connectivity problem occurs, each server processes the full workload of both servers.

- D. During normal operations, the servers split the full load of authentication requests.
- E. During normal operations, each server is used for specific operations, such as device administration and network admission.
- F. The primary servers are used to distribute policy information to other servers in the enterprise.

**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 158**

Which three personas can a Cisco ISE assume in a deployment? (Choose three.)

- A. connection
- B. authentication
- C. administration
- D. testing
- E. policy service
- F. monitoring

**Correct Answer:** CEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 159**

Which three components comprise the Cisco ISE profiler? (Choose three.)

- A. the sensor, which contains one or more probes
- B. the probe manager
- C. a monitoring tool that connects to the Cisco ISE
- D. the trigger, which activates ACLs
- E. an analyzer, which uses configured policies to evaluate endpoints
- F. a remitter tool, which fails over to redundant profilers

**Correct Answer:** ABE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 160**

Which three statements about the Cisco ISE profiler are true? (Choose three.)

- A. It sends endpoint data to AAA servers.
- B. It collects endpoint attributes.
- C. It stores MAC addresses for endpoint systems.
- D. It monitors and polices router and firewall traffic.
- E. It matches endpoints to their profiles.
- F. It stores endpoints in the Cisco ISE database with their profiles.

**Correct Answer: BEF**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 161**

A network administrator needs to determine the ability of existing network devices to deliver key BYOD services. Which tool will complete a readiness assessment and outline hardware and software capable and incapable devices?

- A. Prime Infrastructure
- B. Network Control System
- C. Cisco Security Manager
- D. Identity Services Engine

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 162**

Which EAP method uses a modified version of the MS-CHAP authentication protocol?

- A. EAP-POTP
- B. EAP-TLS
- C. LEAP
- D. EAP-MD5

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 163**

Under which circumstance would an inline posture node be deployed?

- A. When the NAD does not support CoA
- B. When the NAD cannot support the number of connected endpoints
- C. When a PSN is overloaded
- D. To provide redundancy for a PSN

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 164**

Which Cisco ISE 1.x protocol can be used to control admin access to network access devices?

- A. TACACS+
- B. RADIUS
- C. EAP
- D. Kerberos

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 165**

A user is on a wired connection and the posture status is noncompliant.

Which state will their EPS session be placed in?

- A. disconnected
- B. limited
- C. no access
- D. quarantined

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 166**

Which three posture states can be used for authorization rules? (Choose three.)

- A. unknown
- B. known
- C. noncompliant
- D. quarantined
- E. compliant
- F. no access
- G. limited

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 167**

Which two Cisco ISE administration options are available in the Default Posture Status setting? (Choose two.)

- A. Unknown
- B. Compliant
- C. FailOpen
- D. FailClose
- E. Noncompliant

**Correct Answer:** BE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 168**

Which two portals can be configured to use portal FQDN? (Choose two.)

- A. admin
- B. sponsor
- C. guest
- D. my devices
- E. monitoring and troubleshooting

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 169**

Which five portals are provided by PSN? (Choose five.)

- A. guest
- B. sponsor
- C. my devices
- D. blacklist
- E. client provisioning

- F. admin
- G. monitoring and troubleshooting

**Correct Answer:** ABCDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Answer: A, B, C, D, E

#### **QUESTION 170**

When you add a new PSN for guest access services, which two options must be enabled under deployment settings? (Choose two.)

- A. Admin
- B. Monitoring
- C. Policy Service
- D. Session Services
- E. Profiling

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 171**

In Cisco ISE, which probe must be enabled to collect profiling data using Device Sensor?

- A. RADIUS
- B. SNMPQuery
- C. SNMPTrap
- D. Network Scan
- E. Syslog

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 172**

Which two profile attributes can be collected by a Cisco Catalyst Switch that supports Device Sensor? (Choose two.)

- A. LLDP agent information
- B. user agent
- C. DHCP options
- D. open ports
- E. operating system
- F. trunk ports

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 173**

Which two profile attributes can be collected by a Cisco Wireless LAN Controller that supports Device Sensor? (Choose two.)

- A. LLDP agent information
- B. user agent
- C. DHCP options
- D. open ports
- E. CDP agent information
- F. FQDN

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 174**

Which statement about Cisco ISE BYOD is true?

- A. Dual SSID allows EAP-TLS only when connecting to the secured SSID.

- B. Single SSID does not require endpoints to be registered.
- C. Dual SSID allows BYOD for guest users.
- D. Single SSID utilizes open SSID to accommodate different types of users.
- E. Single SSID allows PEAP-MSCHAPv2 for native supplicant provisioning.

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 175**

Which two types of client provisioning resources are used for BYOD implementations? (Choose two.)

- A. user agent
- B. Cisco NAC agent
- C. native supplicant profiles
- D. device sensor
- E. software provisioning wizards

**Correct Answer:** CE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 176**

What is the effect of the ip http secure-server command on a Cisco ISE?

- A. It enables the HTTP server for users to connect on the command line.
- B. It enables the HTTP server for users to connect using Web-based authentication.
- C. It enables the HTTPS server for users to connect using Web-based authentication.
- D. It enables the HTTPS server for users to connect on the command line.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 177**

When RADIUS NAC and AAA Override are enabled for WLC on a Cisco ISE, which two statements about RADIUS NAC are true? (Choose two.)

- A. It will return an access-accept and send the redirection URL for all users.
- B. It establishes secure connectivity between the RADIUS server and the ISE.
- C. It allows the ISE to send a CoA request that indicates when the user is authenticated.
- D. It is used for posture assessment, so the ISE changes the user profile based on posture result.
- E. It allows multiple users to authenticate at the same time.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 178**

What are the initial steps to configure an ACS as a TACACS server?

- A. 1. Choose Network Devices and AAA Clients > Network Resources.  
2. Click Create.
- B. 1. Choose Network Resources > Network Devices and AAA Clients.  
2. Click Create.
- C. 1. Choose Network Resources > Network Devices and AAA Clients.  
2. Click Manage.
- D. 1. Choose Network Devices and AAA Clients > Network Resources.  
2. Click Install.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 179**

Which two statements about administrative access to the Cisco Secure ACS SE are true? (Choose two.)

- A. The Cisco Secure ACS SE supports command-line connections through a serial-port connection.
- B. For GUI access, an administrative GUI user must be created by using the add-guiadmin command.
- C. The Cisco Secure ACS SE supports command-line connections through an Ethernet interface.
- D. An ACL-based policy must be configured to allow administrative-user access.
- E. GUI access to the Cisco Secure ASC SE is not supported.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 180**

When RADIUS NAC and AAA Override are enabled for a WLC on a Cisco ISE, which two statements about RADIUS NAC are true? (Choose two.)

- A. It returns an access-accept and sends the redirection URL for all users.
- B. It establishes secure connectivity between the RADIUS server and the Cisco ISE.
- C. It allows the Cisco ISE to send a CoA request that indicates when the user is authenticated.
- D. It is used for posture assessment, so the Cisco ISE changes the user profile based on posture result.
- E. It allows multiple users to authenticate at the same time.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 181**

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

**Correct Answer:** C

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 182

In an 802.1X authorization process, a network access device provides which three functions? (Choose three.)

- A. Filters traffic prior to authentication
- B. Passes credentials to authentication server
- C. Enforces policy provided by authentication server
- D. Hosts a central web authentication page
- E. Confirms supplicant protocol compliance
- F. Validates authentication credentials

**Correct Answer:** ABC

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 183

Which two switchport commands enable MAB and allow non-802.1X capable devices to immediately run through the MAB process? (Choose two.)

- A. authentication order mab dot1x
- B. authentication order dot1x mab
- C. no authentication timer
- D. dot1x timeout tx-period
- E. authentication open
- F. mab

**Correct Answer:** AF

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 184

Which two attributes must match between two Cisco ASA devices to properly enable high availability? (Choose two.)

- A. model, interface configuration, and RAM
- B. major and minor software release
- C. tcp dead-peer detection protocol
- D. 802.1x authentication identity

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

corrected and valid.

#### **QUESTION 185**

What are two client-side requirements of the NAC Agent and NAC Web Agent installation? (Choose two.)

- A. Administrator workstation rights
- B. Active Directory Domain membership
- C. Allowing of web browser activex installation
- D. WSUS service running

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 186**

In a split ACS deployment with primary and secondary servers, which three statements about AAA load handling are true? (Choose three.)

- A. During normal operations, each server processes the full workload of both servers.
- B. If a AAA connectivity problem occurs, the servers split the full load of authentication requests.
- C. If a AAA connectivity problem occurs, each server processes the full workload of both servers.
- D. During normal operations, the servers split the full load of authentication requests.
- E. During normal operations, each server is used for specific operations, such as device administration and network admission.
- F. The primary servers are used to distribute policy information to other servers in the enterprise.

**Correct Answer:** CDE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 187**

Which three personas can a Cisco ISE assume in a deployment? (Choose three.)

- A. connection
- B. authentication
- C. administration
- D. testing
- E. policy service
- F. monitoring

**Correct Answer:** CEF

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 188**

Which three components comprise the Cisco ISE profiler? (Choose three.)

- A. the sensor, which contains one or more probes
- B. the probe manager
- C. a monitoring tool that connects to the Cisco ISE
- D. the trigger, which activates ACLs
- E. an analyzer, which uses configured policies to evaluate endpoints
- F. a remitter tool, which fails over to redundant profilers

**Correct Answer:** ABE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 189**

Which three statements about the Cisco ISE profiler are true? (Choose three.)

- A. It sends endpoint data to AAA servers.
- B. It collects endpoint attributes.
- C. It stores MAC addresses for endpoint systems.
- D. It monitors and polices router and firewall traffic.
- E. It matches endpoints to their profiles.
- F. It stores endpoints in the Cisco ISE database with their profiles.

**Correct Answer:** BEF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 190**

From which location can you run reports on endpoint profiling?

- A. Reports > Operations > Catalog > Endpoint
- B. Operations > Reports > Catalog > Endpoint
- C. Operations > Catalog > Reports > Endpoint
- D. Operations > Catalog > Endpoint

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 191**

Which two services are included in the Cisco ISE posture service? (Choose two.)

- A. posture administration
- B. posture run-time
- C. posture monitoring
- D. posture policing

E. posture catalog

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 192

What is a requirement for posture administration services in Cisco ISE?

- A. at least one Cisco router to store Cisco ISE profiling policies
- B. Cisco NAC Agents that communicate with the Cisco ISE server
- C. an ACL that points traffic to the Cisco ISE deployment
- D. the advanced license package must be installed

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 193

Which two statements about Cisco NAC Agents that are installed on clients that interact with the Cisco ISE profiler are true? (Choose two.)

- A. They send endpoint data to AAA servers.
- B. They collect endpoint attributes.
- C. They interact with the posture service to enforce endpoint security policies.
- D. They block access from the network through noncompliant endpoints.
- E. They store endpoints in the Cisco ISE with their profiles.
- F. They evaluate clients against posture policies, to enforce requirements.

**Correct Answer:** CF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 194**

What steps must you perform to deploy a CA-signed identify certificate on an ISE device?

- A. 1. Download the CA server certificate.  
2. Generate a signing request and save it as a file.  
3. Access the CA server and submit the ISE request.  
4. Install the issued certificate on the ISE.
- B. 1. Download the CA server certificate.  
2. Generate a signing request and save it as a file.  
3. Access the CA server and submit the ISE request.  
4. Install the issued certificate on the CA server.
- C. 1. Generate a signing request and save it as a file.  
2. Download the CA server certificate.  
3. Access the ISE server and submit the CA request.  
4. Install the issued certificate on the CA server.
- D. 1. Generate a signing request and save it as a file.  
2. Download the CA server certificate.  
3. Access the CA server and submit the ISE request.  
4. Install the issued certificate on the ISE.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 195**

What implementation must be added to the WLC to enable 802.1X and CoA for wireless endpoints?

- A. the ISE
- B. an ACL
- C. a router
- D. a policy server

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 196**

From which location can you run reports on endpoint profiling?

- A. Reports > Operations > Catalog > Endpoint
- B. Operations > Reports > Catalog > Endpoint
- C. Operations > Catalog > Reports > Endpoint
- D. Operations > Catalog > Endpoint

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 197**

Which two services are included in the Cisco ISE posture service? (Choose two.)

- A. posture administration
- B. posture run-time
- C. posture monitoring
- D. posture policing
- E. posture catalog

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 198**

What is a requirement for posture administration services in Cisco ISE?

- A. at least one Cisco router to store Cisco ISE profiling policies
- B. Cisco NAC Agents that communicate with the Cisco ISE server
- C. an ACL that points traffic to the Cisco ISE deployment
- D. the advanced license package must be installed

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 199**

Which two statements about Cisco NAC Agents that are installed on clients that interact with the Cisco ISE profiler are true? (Choose two.)

- A. They send endpoint data to AAA servers.
- B. They collect endpoint attributes.
- C. They interact with the posture service to enforce endpoint security policies.
- D. They block access from the network through noncompliant endpoints.
- E. They store endpoints in the Cisco ISE with their profiles.
- F. They evaluate clients against posture policies, to enforce requirements.

**Correct Answer:** CF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 200**

What steps must you perform to deploy a CA-signed identify certificate on an ISE device?

- A.
  1. Download the CA server certificate.
  2. Generate a signing request and save it as a file.
  3. Access the CA server and submit the ISE request.
  4. Install the issued certificate on the ISE.
- B.
  1. Download the CA server certificate.
  2. Generate a signing request and save it as a file.
  3. Access the CA server and submit the ISE request.
  4. Install the issued certificate on the CA server.
- C.
  1. Generate a signing request and save it as a file.
  2. Download the CA server certificate.
  3. Access the ISE server and submit the CA request.
  4. Install the issued certificate on the CA server.
- D.
  1. Generate a signing request and save it as a file.

2. Download the CA server certificate.
3. Access the CA server and submit the ISE request.
4. Install the issued certificate on the ISE.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 201**

What implementation must be added to the WLC to enable 802.1X and CoA for wireless endpoints?

- A. the ISE
- B. an ACL
- C. a router
- D. a policy server

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 202**

What are the initial steps must you perform to add the ISE to the WLC?

- A.
  1. With a Web browser, establish an HTTP connection to the WLC pod.
  2. Navigate to Administration > Authentication > New.
  3. Enter server values to begin the configuration.
- B.
  1. With a Web browser, establish an FTP connection to the WLC pod.
  2. Navigate to Security > Administration > New.
  3. Add additional security features for FTP authentication.
- C.
  1. With a Web browser, establish an HTTP connection to the WLC pod.
  2. Navigate to Authentication > New.
  3. Enter ACLs and Authentication methods to begin the configuration.
- D.
  1. With a Web browser connect, establish an HTTPS connection to the WLC pod.
  2. Navigate to Security > Authentication > New.
  3. Enter server values to begin the configuration.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 203**

Which command configures console port authorization under line con 0?

- A. authorization default|WORD
- B. authorization exec line con 0|WORD
- C. authorization line con 0|WORD
- D. authorization exec default|WORD

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 204**

Which two statements about administrative access to the ACS Solution Engine are true? (Choose two.)

- A. The ACS Solution Engine supports command-line connections through a serial-port connection.
- B. For GUI access, an administrative GUI user must be created with the add-guiadmin command.
- C. The ACS Solution Engine supports command-line connections through an Ethernet interface.
- D. An ACL-based policy must be configured to allow administrative-user access.
- E. GUI access to the ACS Solution Engine is not supported.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 205**

What is the purpose of the Cisco ISE Guest Service Sponsor Portal?

- A. It tracks and stores user activity while connected to the Cisco ISE.
- B. It securely authenticates guest users for the Cisco ISE Guest Service.
- C. It filters guest users from account holders to the Cisco ISE.
- D. It creates and manages Guest User accounts.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 206**

Which protocol sends authentication and accounting in different requests?

- A. RADIUS
- B. TACACS+
- C. EAP-Chaining
- D. PEAP
- E. EAP-TLS

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 207**

You enabled the guest session limit feature on the Cisco ISE. However, end users report that the same guest can log in from multiple devices simultaneously.

Which configuration is missing on the network access device?

- A. RADIUS authentication
- B. RADIUS accounting
- C. DHCP required
- D. AAA override

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 208**

A properly configured Cisco ISE Policy Service node is not receiving any profile data from a Cisco switch that runs Device Sensor.

Which option is the most likely reason for the failure?

- A. Syslog is configured for the Policy Administration Node.
- B. RADIUS Accounting is disabled.
- C. The SNMP community strings are mismatched.
- D. RADIUS Authentication is misconfigured.
- E. The connected endpoints support CDP but not DHCP.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 209**

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 210**

In an 802.1X authorization process, a network access device provides which three functions? (Choose three.)

- A. Filters traffic prior to authentication
- B. Passes credentials to authentication server
- C. Enforces policy provided by authentication server
- D. Hosts a central web authentication page
- E. Confirms supplicant protocol compliance
- F. Validates authentication credentials

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 211

Which two switchport commands enable MAB and allow non-802.1X capable devices to immediately run through the MAB process? (Choose two.)

- A. authentication order mab dot1x
- B. authentication order dot1x mab
- C. no authentication timer
- D. dot1x timeout tx-period
- E. authentication open
- F. mab

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 212

Which two attributes must match between two Cisco ASA devices to properly enable high availability? (Choose two.)

- A. model, interface configuration, and RAM
- B. major and minor software release
- C. tcp dead-peer detection protocol

D. 802.1x authentication identity

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 213**

What are two client-side requirements of the NAC Agent and NAC Web Agent installation? (Choose two.)

- A. Administrator workstation rights
- B. Active Directory Domain membership
- C. Allowing of web browser activex installation
- D. WSUS service running

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 214**

Which three algorithms should be avoided due to security concerns? (Choose three.)

- A. DES for encryption
- B. SHA-1 for hashing
- C. 1024-bit RSA
- D. AES GCM mode for encryption
- E. HMAC-SHA-1
- F. 256-bit Elliptic Curve Diffie-Hellman
- G. 2048-bit Diffie-Hellman

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 215**

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 216**

Which Cisco ASDM option configures WebVPN access on a Cisco ASA?

- A. Configuration > WebVPN > WebVPN Access
- B. Configuration > Remote Access VPN > Clientless SSL VPN Access
- C. Configuration > WebVPN > WebVPN Config
- D. Configuration > VPN > WebVPN Access

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 217**

A user with IP address 10.10.10.10 is unable to access a HTTP website at IP address 209.165.200.225 through a Cisco ASA. Which two features and commands will help troubleshoot the issue? (Choose two.)

- A. Capture user traffic using command capture capin interface inside match ip host 10.10.10.10 any
- B. After verifying that user traffic reaches the firewall using syslogs or captures, use packet tracer command packet-tracer input inside tcp 10.10.10.10 1234 209.165.200.225 80
- C. Enable logging at level 1 and check the syslogs using commands logging enable, logging buffered 1 and show logging | include 10.10.10.10

- D. Check if an access-list on the firewall is blocking the user by using command `show running- config access-list | include 10.10.10.10`
- E. Use packet tracer command `packet-tracer input inside udp 0.10.10.10 1234192.168.1.3 161` to see what the firewall is doing with the user's traffic

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 218

A Cisco router may have a fan issue that could increase its temperature and trigger a failure. What troubleshooting steps would verify the issue without causing additional risks?

- A. Configure logging using commands "logging on", "logging buffered 4", and check for fan failure logs using "show logging"
- B. Configure logging using commands "logging on", "logging buffered 6", and check for fan failure logs using "show logging"
- C. Configure logging using commands "logging on", "logging discriminator msglog1 console 7", and check for fan failure logs using "show logging"
- D. Configure logging using commands "logging host 10.11.10.11", "logging trap 2", and check for fan failure logs at the syslog server 10.11.10.11

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 219

An internet-based VPN solution is being considered to replace an existing private WAN connecting remote offices. A multimedia application is used that relies on multicast for communication. Which two VPN solutions meet the application's network requirement? (Choose two.)

- A. FlexVPN
- B. DMVPN
- C. Group Encrypted Transport VPN
- D. Crypto-map based Site-to-Site IPsec VPNs
- E. AnyConnect VPN

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 220**

A private wan connection is suspected of intermittently corrupting data. Which technology can a network administrator use to detect and drop the altered data traffic?

- A. AES-128
- B. RSA Certificates
- C. SHA2-HMAC
- D. 3DES
- E. Diffie-Helman Key Generation

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 221**

A company needs to provide secure access to its remote workforce. The end users use public kiosk computers and a wide range of devices. They will be accessing only an internal web application. Which VPN solution satisfies these requirements?

- A. Clientless SSLVPN
- B. AnyConnect Client using SSLVPN
- C. AnyConnect Client using IKEv2
- D. FlexVPN Client
- E. Windows built-in PPTP client

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

valid.

**QUESTION 222**

A network administrator is configuring AES encryption for the ISAKMP policy on an IOS router. Which two configurations are valid? (Choose two.)

- A. crypto isakmp policy 10  
encryption aes 254
- B. crypto isakmp policy 10  
encryption aes 192
- C. crypto isakmp policy 10  
encryption aes 256
- D. crypto isakmp policy 10  
encryption aes 196
- E. crypto isakmp policy 10  
encryption aes 199
- F. crypto isakmp policy 10  
encryption aes 64

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 223**

Which two qualify as Next Generation Encryption integrity algorithms? (Choose two.)

- A. SHA-512
- B. SHA-256
- C. SHA-192
- D. SHA-380
- E. SHA-192
- F. SHA-196

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 224**

Which statement is true when implementing a router with a dynamic public IP address in a crypto map based site-to-site VPN?

- A. The router must be configured with a dynamic crypto map.
- B. Certificates are always used for phase 1 authentication.
- C. The tunnel establishment will fail if the router is configured as a responder only.
- D. The router and the peer router must have NAT traversal enabled.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 225**

Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect? (Choose two.)

- A. The VPN server must have a self-signed certificate.
- B. A SSL group pre-shared key must be configured on the server.
- C. Server side certificate is optional if using AAA for client authentication.
- D. The VPN IP address pool can overlap with the rest of the LAN networks.
- E. DTLS can be enabled for better performance.

**Correct Answer:** DE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 226**

Which two are valid ISE posture conditions? (Choose two.)

- A. Dictionary
- B. memberOf
- C. Profile status
- D. File
- E. Service

**Correct Answer:** DE

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 227**

A network engineer is configuring HTTP based CWA on a switch. Which three configuration elements are required? (Choose three.)

- A. HTTP server enabled
- B. Radius authentication on the port with MAB
- C. Redirect access-list
- D. Redirect-URL
- E. HTTP secure server enabled
- F. Radius authentication on the port with 802.1x
- G. Pre-auth port based access-list

**Correct Answer:** ABC

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 228**

Which three statements describe differences between TACACS+ and RADIUS? (Choose three.)

- A. RADIUS encrypts the entire packet, while TACACS+ encrypts only the password.
- B. TACACS+ encrypts the entire packet, while RADIUS encrypts only the password.
- C. RADIUS uses TCP, while TACACS+ uses UDP.
- D. TACACS+ uses TCP, while RADIUS uses UDP.
- E. RADIUS uses ports 1812 and 1813, while TACACS+ uses port 49.
- F. TACACS+ uses ports 1812 and 1813, while RADIUS uses port 49

**Correct Answer:** BDE

**Section:** (none)

**Explanation****Explanation/Reference:**

**QUESTION 229**

Which two identity store options allow you to authorize based on group membership? (Choose two).

- A. Lightweight Directory Access Protocol
- B. RSA SecurID server
- C. RADIUS
- D. Active Directory

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 230**

What attribute could be obtained from the SNMP query probe?

- A. FQDN
- B. CDP
- C. DHCP class identifier
- D. User agent

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 231**

What is a required configuration step for an 802.1X capable switch to support dynamic VLAN and ACL assignments?

- A. Configure the VLAN assignment.
- B. Configure the ACL assignment.
- C. Configure 802.1X authenticator authorization.
- D. Configure port security on the switch port.

**Correct Answer:** C

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 232

Which network component would issue the CoA?

- A. switch
- B. endpoint
- C. Admin Node
- D. Policy Service Node

**Correct Answer:** D

**Section:** (none)

### Explanation

### Explanation/Reference:

#### QUESTION 233

What steps must you perform to deploy a CA-signed identity certificate on an ISE device?

- A.
  1. Download the CA server certificate and install it on ISE.
  2. Generate a signing request and save it as a file.
  3. Access the CA server and submit the CA request.
  4. Install the issued certificate on the ISE.
- B.
  1. Download the CA server certificate and install it on ISE.
  2. Generate a signing request and save it as a file.
  3. Access the CA server and submit the CSR.
  4. Install the issued certificate on the CA server.
- C.
  1. Generate a signing request and save it as a file.
  2. Download the CA server certificate and install it on ISE.
  3. Access the ISE server and submit the CA request.
  4. Install the issued certificate on the CA server.
- D.
  1. Generate a signing request and save it as a file.
  2. Download the CA server certificate and install it on ISE.
  3. Access the CA server and submit the CSR.
  4. Install the issued certificate on the ISE.

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 234**

An organization has recently deployed ISE with Trustsec capable Cisco switches and would like to allow differentiated network access based on user groups. Which solution is most suitable for achieving these goals?

- A. Cyber Threat Defense for user group control by leveraging Netflow exported from the Cisco switches and identity information from ISE
- B. MACsec in Multiple-Host Mode in order to encrypt traffic at each hop of the network infrastructure
- C. Identity-based ACLs preconfigured on the Cisco switches with user identities provided by ISE
- D. Cisco Security Group Access Policies to control access based on SGTs assigned to different user groups

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 235**

Which three are required steps to enable SXP on a Cisco ASA? (Choose three).

- A. configure AAA authentication
- B. configure password
- C. issue the aaa authorization command aaa-server group command
- D. configure a peer
- E. configure TACACS
- F. issue the cts sxp enable command

**Correct Answer: BDF**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 236**

Which three algorithms should be avoided due to security concerns? (Choose three.)

- A. DES for encryption
- B. SHA-1 for hashing
- C. 1024-bit RSA
- D. AES GCM mode for encryption
- E. HMAC-SHA-1
- F. 256-bit Elliptic Curve Diffie-Hellman
- G. 2048-bit Diffie-Hellman

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

answer is corrected.

#### **QUESTION 237**

In the command 'aaa authentication default group tacacs local', how is the word 'default' defined?

- A. Command set
- B. Group name
- C. Method list
- D. Login type

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 238**

Which statement about IOS accounting is true?

- A. A named list of AAA methods must be defined.
- B. A named list of accounting methods must be defined.
- C. Authorization must be configured before accounting.
- D. A named list of tracking methods must be defined.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 239**

What are the initial steps to configure an ACS as a TACACS server?

- A. 1. Choose Network Devices and AAA Clients > Network Resources.  
2. Click Create.
- B. 1. Choose Network Resources > Network Devices and AAA Clients.  
2. Click Create.
- C. 1. Choose Network Resources > Network Devices and AAA Clients.  
2. Click Manage.
- D. 1. Choose Network Devices and AAA Clients > Network Resources.  
2. Click Install.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 240**

Which effect does the ip http secure-server command have on a Cisco ISE?

- A. It enables the HTTP server for users to connect on the command line.
- B. It enables the HTTP server for users to connect by using web-based authentication.
- C. It enables the HTTPS server for users to connect by using web-based authentication.
- D. It enables the HTTPS server for users to connect on the command line.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 241**

Which three pieces of information can be found in an authentication detail report? (Choose three.)

- A. DHCP vendor ID
- B. user agent string
- C. the authorization rule matched by the endpoint
- D. the EAP method the endpoint is using
- E. the RADIUS username being used
- F. failed posture requirement

**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 242**

Certain endpoints are missing DHCP profiling data.

Which option describes what can be used to determine if DHCP requests from clients are reaching Cisco ISE?

- A. output of show interface gigabitEthernet 0 from the CLI
- B. output of debug logging all 7 from the CLI
- C. output of show logging application profiler.log from the CLI
- D. the TCP dump diagnostic tool through the GUI
- E. the posture troubleshooting diagnostic tool through the GUI

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 243**

Which debug command on a Cisco WLC shows the reason that a client session was terminated?

- A. debug dot11 state enable

- B. debug dot1x packet enable
- C. debug client mac addr
- D. debug dtls event enable
- E. debug ap enable cisco ap

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 244**

Which two identity databases are supported when PEAP-MSCHAPv2 is used as EAP type? (Choose two.)

- A. Windows Active Directory
- B. LDAP
- C. RADIUS token server
- D. internal endpoint store
- E. internal user store
- F. certificate authentication profile
- G. RSA SecurID

**Correct Answer:** AE

**Section:** (none)

**Explanation**

**Explanation/Reference:**