Cisco 300-208

Implementing Cisco Secure Access Solutions

Version: 5.0

QUESTION NO: 1

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

Answer: A
Explanation:

QUESTION NO: 2

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

Answer: A
Explanation:

QUESTION NO: 3

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

Answer: C
Explanation:

QUESTION NO: 4

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

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

Answer: A
Explanation:

QUESTION NO: 5

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

Answer: C
Explanation:

QUESTION NO: 6

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

Answer: A
Explanation:

QUESTION NO: 7

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

Answer: B

Explanation:

QUESTION NO: 8

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

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

Answer: D,E

Explanation:

QUESTION NO: 9

Refer to the exhibit.

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.

Answer: B,C,F
Explanation:

QUESTION NO: 10

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.

Answer: B
Explanation:

QUESTION NO: 11

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

Answer: A
Explanation:

QUESTION NO: 12

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

Answer: C

Explanation:

QUESTION NO: 13

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

Answer: A,C,D
Explanation:

QUESTION NO: 14

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

Answer: B
Explanation:

QUESTION NO: 15

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

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

Answer: C

Explanation:

QUESTION NO: 16

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.

Answer: A
Explanation:

QUESTION NO: 17

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

Answer: B,C,E
Explanation:

QUESTION NO: 18

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

Answer: D
Explanation:

QUESTION NO: 19

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.

Answer: C
Explanation:

QUESTION NO: 20

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

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

Answer: A
Explanation:

QUESTION NO: 21

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

Answer: A

Explanation:

QUESTION NO: 22

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

Answer: B,D,F

Explanation:

QUESTION NO: 23

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

Answer: C

Explanation:

QUESTION NO: 24

Refer to the exhibit.

If the given configuration is applied to the object-group vpnservers, 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.

Answer: D
Explanation:

QUESTION NO: 25

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

Answer: A
Explanation:

QUESTION NO: 26

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

Answer: C
Explanation:

QUESTION NO: 27

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

Answer: C
Explanation:

QUESTION NO: 28

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

Answer: A
Explanation:

QUESTION NO: 29

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

Answer: A
Explanation:

QUESTION NO: 30

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.

Answer: D
Explanation:

QUESTION NO: 31

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

Answer: B,C,D
Explanation:

QUESTION NO: 32

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

Answer: A,B
Explanation:

QUESTION NO: 33

What is another term for 802.11i wireless network security?

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

Answer: E
Explanation:

QUESTION NO: 34

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

Answer: A,B
Explanation:

QUESTION NO: 35

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

Answer: A
Explanation:

QUESTION NO: 36

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

Answer: A
Explanation:

QUESTION NO: 37

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.

Answer: B
Explanation:

QUESTION NO: 38

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

Answer: B,D

Explanation:

QUESTION NO: 39

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.

Answer: D

Explanation:

QUESTION NO: 40

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.

Answer: B,C,D

Explanation:

QUESTION NO: 41

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

Answer: A,B,D

Explanation:

QUESTION NO: 42

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.

Answer: C,D,E

Explanation:

QUESTION NO: 43

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

Answer: C,E,F

Explanation:

QUESTION NO: 44

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

Answer: A,B,E
Explanation:

QUESTION NO: 45

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.

Answer: B,E,F
Explanation:

QUESTION NO: 46

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

Answer: B
Explanation:

QUESTION NO: 47

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

Answer: A,B

Explanation:

QUESTION NO: 48

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

Answer: D

Explanation:

QUESTION NO: 49

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.

Answer: C,F

Explanation:

QUESTION NO: 50

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.

Answer: D

Explanation:

QUESTION NO: 51

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

Answer: A

Explanation:

QUESTION NO: 52

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.

Answer: D
Explanation:

QUESTION NO: 53

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

Answer: D
Explanation:

QUESTION NO: 54

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.

Answer: B,D

Explanation:

QUESTION NO: 55

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.

Answer: D

Explanation:

QUESTION NO: 56

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.

Answer: C

Explanation:

QUESTION NO: 57

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.

Answer: C,D

Explanation:

QUESTION NO: 58

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.

Answer: B

Explanation:

QUESTION NO: 59

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.

Answer: B,D

Explanation:

QUESTION NO: 60

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.

Answer: C,D

Explanation:

QUESTION NO: 61

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

Answer: C

Explanation:

QUESTION NO: 62

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

Answer: A,B,C

Explanation:

QUESTION NO: 63

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

Answer: A,F
Explanation:

QUESTION NO: 64

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

Answer: A,B
Explanation:

QUESTION NO: 65

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

Answer: A,C
Explanation:

QUESTION NO: 66

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

Answer: A,B,C
Explanation:

QUESTION NO: 67

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

Answer: C
Explanation:

QUESTION NO: 68

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.

Answer: C
Explanation:

QUESTION NO: 69

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.

Answer: B
Explanation:

QUESTION NO: 70

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.

Answer: C
Explanation:

QUESTION NO: 71

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

Answer: B
Explanation:

QUESTION NO: 72

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

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

Answer: D,E
Explanation:

QUESTION NO: 73

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

Answer: A,B,C
Explanation:

QUESTION NO: 74

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

Answer: B,D,E
Explanation:

QUESTION NO: 75

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

Answer: A,D
Explanation:

QUESTION NO: 76

What attribute could be obtained from the SNMP query probe?

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

Answer: B
Explanation:

QUESTION NO: 77

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.

Answer: C
Explanation:

QUESTION NO: 78

Which network component would issue the CoA?

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

Answer: D
Explanation:

QUESTION NO: 79

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.

Answer: D

Explanation:

QUESTION NO: 80

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

Answer: D

Explanation:

QUESTION NO: 81

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

Answer: B,D,F

Explanation:

QUESTION NO: 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

Answer: B,C,E
Explanation:

QUESTION NO: 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

Answer: B
Explanation:

QUESTION NO: 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

Answer: C,E
Explanation:

QUESTION NO: 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

Answer: A,D

Explanation:

QUESTION NO: 86

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

Answer: C,D,E

Explanation:

QUESTION NO: 87

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

Answer: D
Explanation:

QUESTION NO: 88

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

Answer: C
Explanation:

QUESTION NO: 89

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

Answer: A,E
Explanation:

QUESTION NO: 90

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

Answer: A,B
Explanation:

QUESTION NO: 91

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

Answer: B
Explanation:

QUESTION NO: 92

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

Answer: B
Explanation:

QUESTION NO: 93

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

Answer: C
Explanation:

QUESTION NO: 94

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

Answer: C
Explanation:

QUESTION NO: 95

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

Answer: B
Explanation:

QUESTION NO: 96

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

Answer: A,B
Explanation:

QUESTION NO: 97

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.

Answer: A
Explanation:

QUESTION NO: 98

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

Answer: A
Explanation:

QUESTION NO: 99

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

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

D. PEAP

Answer: A
Explanation:

QUESTION NO: 100

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

Answer: B
Explanation:

QUESTION NO: 101

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

Answer: A
Explanation:

QUESTION NO: 102

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

A. EAP-POTP
B. EAP-TLS

C. LEAP
D. EAP-MD5

Answer: C
Explanation:

QUESTION NO: 103

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

Answer: A
Explanation:

QUESTION NO: 104

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

Answer: B
Explanation:

QUESTION NO: 105

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

Answer: D
Explanation:

QUESTION NO: 106

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

Answer: A,C,E
Explanation:

QUESTION NO: 107

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

Answer: B,E
Explanation:

QUESTION NO: 108

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

Answer: B,D

Explanation:

QUESTION NO: 109

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

Answer: A,B,C,D,E

Explanation:

QUESTION NO: 110

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

Answer: C,D

Explanation:

QUESTION NO: 111

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

Answer: A

Explanation:

QUESTION NO: 112

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

Answer: A,C

Explanation:

QUESTION NO: 113

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

Answer: B,C

Explanation:

QUESTION NO: 114

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.

Answer: E
Explanation:

QUESTION NO: 115

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

Answer: C,E
Explanation:

QUESTION NO: 116

Which protocol sends authentication and accounting in different requests?

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

Answer: B

Explanation:

QUESTION NO: 117

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

Answer: B

Explanation:

QUESTION NO: 118

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.

Answer: B

Explanation:

QUESTION NO: 119 DRAG DROP

Answer:

Explanation: