

# Cisco

## Exam 300-208

### Implementing Cisco Secure Access Solutions

Version: 10.0

[ Total Questions: 224 ]

**Question No : 1**

With which two appliance-based products can Cisco Prime Infrastructure integrate to perform centralized management? (Choose two.)

- A. Cisco Managed Services Engine
- B. Cisco Email Security Appliance
- C. Cisco Wireless Location Appliance
- D. Cisco Content Security Appliance
- E. Cisco ISE

**Answer: A,E**

**Question No : 2**

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**

**Question No : 3**

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**

**Question No : 4**

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**

**Question No : 5**

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**

**Question No : 6**

Which option is the correct format of username in MAB authentication?

- A. host/LSB67.cisco.com
- B. chris@cisco.com
- C. 10:41:7F:46:9F:89
- D. CISCO\chris

**Answer: C**

**Question No : 7**

When you configure an endpoint profiling policy rule, which option describes the purpose of the minimum certainty factor?

- A. It is compared to the total certainty metric of an individual endpoint to determine whether the endpoint can be trusted.
- B. It is compared to the assigned certainty value of an individual endpoint in a device database to determine whether the endpoint can be trusted.
- C. It is used to compare the policy condition to other active policies.
- D. It is used to determine the likelihood that an endpoint is an active, trusted device on the network.

**Answer: A**

**Question No : 8**

What is the function of the SGACL policy matrix on a Cisco TrustSec domain with SGT Assignment?

- A. It determines which access policy to apply to the endpoint.
- B. It determines which switches are trusted within the TrustSec domain.
- C. It determines the path the SGT of the packet takes when entering the Cisco TrustSec domain.
- D. It lists all servers that are permitted to participate in the TrustSec domain.
- E. It lists all hosts that are permitted to participate in the TrustSec domain.

**Answer: A**

**Question No : 9**

You have configured a Cisco ISE 1.2 deployment for self-registration of guest users. What two options can you select from to determine when the account duration timer begins? (Choose two.)

- A. CreateTime
- B. FirstLogin
- C. BeginLogin
- D. StartTime

**Answer: A,B**

**Question No : 10**

Which type of access list is the most scalable that Cisco ISE can use to implement network authorization enforcement for a large number of users?

- A. downloadable access lists
- B. named access lists
- C. VLAN access lists
- D. MAC address access lists

**Answer: A**

**Question No : 11**

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**

**Question No : 12**

Which attribute is needed for Cisco ISE to profile a device with HTTP probe?

- A. user-agent
- B. OUI
- C. host-name
- D. cdp-cache-platform
- E. dhcp-class-identifier
- F. sysDescr

**Answer: A**

**Question No : 13**

You configured wired 802.1X with EAP-TLS on Windows machines. The ISE authentication detail report shows "EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain." What is the most likely cause of this error?

- A. The ISE certificate store is missing a CA certificate.
- B. The Wireless LAN Controller is missing a CA certificate.
- C. The switch is missing a CA certificate.
- D. The Windows Active Directory server is missing a CA certificate.

**Answer: A**

**Question No : 14**

When you select Centralized Web Auth in the ISE Authorization Profile, which two components host the web authentication portal? (Choose two.)

- A. ISE
- B. the WLC
- C. the access point
- D. the switch
- E. the endpoints

**Answer: B,D**

**Question No : 15**

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**

**Question No : 16**

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**

**Question No : 17**

A user configured a Cisco Identity Service Engine and switch to work with downloadable access list for wired dot1x users, though it is failing to work. Which command must be added to address the issue?

- A. ip dhcp snooping
- B. ip device tracking
- C. dot1x pae authenticator
- D. aaa authentication dot1x default group radius

**Answer: B**

**Question No : 18**

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**

**Question No : 19**

By default, how many days does Cisco ISE wait before it purges the expired guest accounts?

- A. 1
- B. 10
- C. 15
- D. 20

**Answer: C**

**Question No : 20**

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**

**Question No : 21**

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**



**Question No : 22**

What EAP method supports mutual certificate-based authentication?

- A. EAP-TTLS
- B. EAP-MSCHAP
- C. EAP-TLS
- D. EAP-MD5

**Answer: C**

**Question No : 23**

Which profiling capability allows you to gather and forward network packets to an analyzer?

- A. collector
- B. spanner
- C. retriever
- D. aggregator

**Answer: A**

**Question No : 24**

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**

**Question No : 25**

Which network component would issue the CoA?

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

**Answer: D**

**Question No : 26**

Which option is the correct redirect-ACL for Wired-CWA, with 10.201.228.76 being the Cisco ISE IP address?

- A. ip access-l ex ACL-WEBAUTH-REDIRECT deny udp any any eq domain deny ip any host 10.201.228.76 permit tcp any any eq 80 permit tcp any any eq 443
- B. ip access-l ex ACL-WEBAUTH-REDIRECT permit udp any any eq domain permit ip any host 10.201.228.76 deny tcp any any eq 80 permit tcp any any eq 443
- C. ip access-l ex ACL-WEBAUTH-REDIRECT deny udp any any eq domain permit tcp any host 10.201.228.76 eq 8443 deny ip any host 10.201.228.76 permit tcp any any eq 80 permit tcp any any eq 443
- D. ip access-l ex ACL-WEBAUTH-REDIRECT permit udp any any eq domain deny ip any host 10.201.228.76 permit tcp any any eq 80 permit tcp any any eq 443

**Answer: A**

**Question No : 27**

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