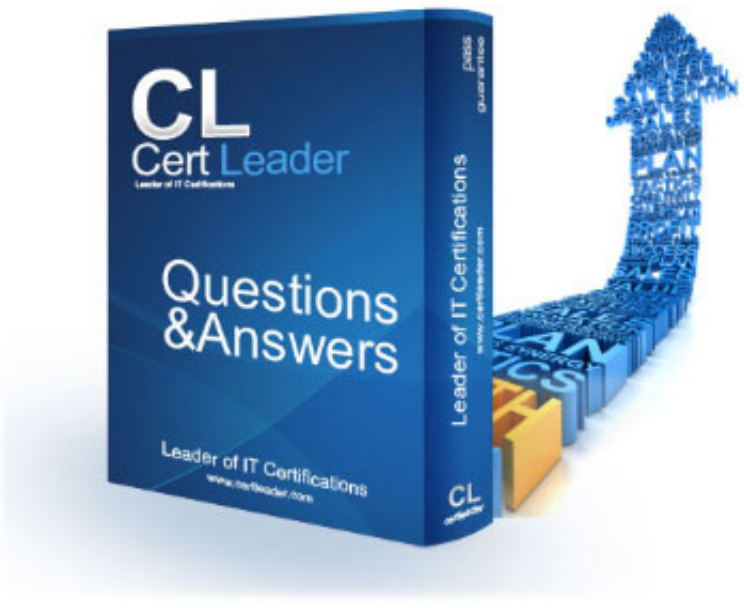
300-375 Dumps

Securing Cisco Wireless Enterprise Networks

https://www.certleader.com/300-375-dumps.html



NEW QUESTION 1
Which two 802.11 methods can be configured to protect card holder data? (Choose two.)

A. CCMP
B. WEP
C. SSL
D. TKIP
E. VPN

Answer: CE

Explanation:

NEW QUESTION 2
An engineer is changing the authentication method of a wireless network from EAP-FAST to EAP-TLS. Which two changes are necessary? (Choose two.)

A. Cisco Secure ACS is required.
B. A Cisco NAC server is required.
C. All authentication clients require their own certificates.
D. The authentication server now requires a certificate.
E. The users require the Cisco AnyConnect clien

Answer: CD

Explanation:

NEW QUESTION 3
Which mobility mode must a Cisco 5508 wireless Controller be in to use the MA functionality on a cisco catalyst 3850 series switch with a cisco 550 Wireless Controller as an MC?

A. classic mobility
B. new mobility
C. converged access mobility
D. auto-anchor mobility

Answer: C

Explanation:

NEW QUESTION 4
When you configure BYOD access to the network, you face increased security risks and challenges. Which challenge is resolved by deploying digital client certificates?

A. managing the increase connected devices
B. ensuring wireless LAN performance and reliability
C. providing device choice and support
D. enforcing company usage policies

Answer: D

Explanation:

NEW QUESTION 5
Refer to the exhibit.

What is the 1.1.1.1 IP address?

A. the wireless client IP address
B. the RADIUS server IP address
C. the controller management IP address
D. the lightweight IP address
E. the controller AP-manager IP address
F. the controller virtual interface IP address

Answer: F

Explanation:

NEW QUESTION 6
A Customer is concerned about denial of service attacks that impair the stable operation of the corporate wireless network. The customer wants to purchase mobile devices that will operate on the corporate wireless network. Which IEEE standard should the mobile devices support to address the customer concerns?

A. 802.11w
B. 802.11k
C. 802.11r
D. 802.11h

Answer: A

Explanation:

NEW QUESTION 7
An engineer is configuring client MFP. What WLAN Layer 2 security must be selected to use client MFP?

A. Static WEP
B. CKIP
C. WPA+WPA2
D. 802 1x

Answer: C

Explanation:

NEW QUESTION 8
Which CLI command do you use on Cisco IOS XE Software to put the AP named Floor1_AP1 back in the default AP group?

A. ap Floor1_AP1 ap-groupname default-group
B. ap name Floor1_AP1 apgroup default-group
C. ap name Floor1_AP1 ap-groupname default-group
D. ap name Floor1_AP1 ap-groupname default

Answer: C

Explanation:

NEW QUESTION 9
An engineer is configuring a new mobility anchor for a WLAN on the CLI with the config wlan mobility anchor add 3 10.10.10.10 command, but the command is failing. Which two conditions must be met to be able to enter this command? (Choose two.)

A. The anchor controller IP address must be within the management interface subnet.
B. The anchor controller must be in the same mobility group.
C. The WLAN must be enabled.
D. The mobility group keepalive must be configured.
E. The indicated WLAN ID must be present on the controlle

Answer: AB

Explanation:

NEW QUESTION 10
A customer has deployed PEAP authentication with a Novell eDirectory LDAP Server. Which authentication method must be configured on the client to support this deployment?

A. PEAP(EAP-MSCHAPv2)
B. PEAP(EAP-TTLS)
C. PEAP(EAP-GTC)
D. PEAP(EAP-WPA)

Answer: C

Explanation:

NEW QUESTION 10
Access points at branch sites for a company are in FlexConncct mode and perform local switching, but they authenticate to the central RADIUS at headquarters. VPN connections to the headquarters have gone down, but each branch site has a local authentication server. Which three features on the wireless controller can be configured to maintain network operations if this situation reoccurs? (Choose three.)

A. Put APs in FlexConnect Group for Remote Branches.
B. Set Branch RADIUS as Primary.
C. Put APs in AP Group Per Branch.

D. Put APs in FlexConnect Group Per Branch.
E. Set Branch RADIUS OS Secondary.
F. Set HQ RADIUS a-s primar

Answer: AEF

Explanation:

NEW QUESTION 13
Which security method does a Cisco guest wireless deployment that relies on Cisco ISE guest portal for user authentication use?

A. Layer 2 and Layer 3
B. Layer 2 only
C. No security methods are needed to deploy CWA
D. Layer 3 only

Answer: B

Explanation:

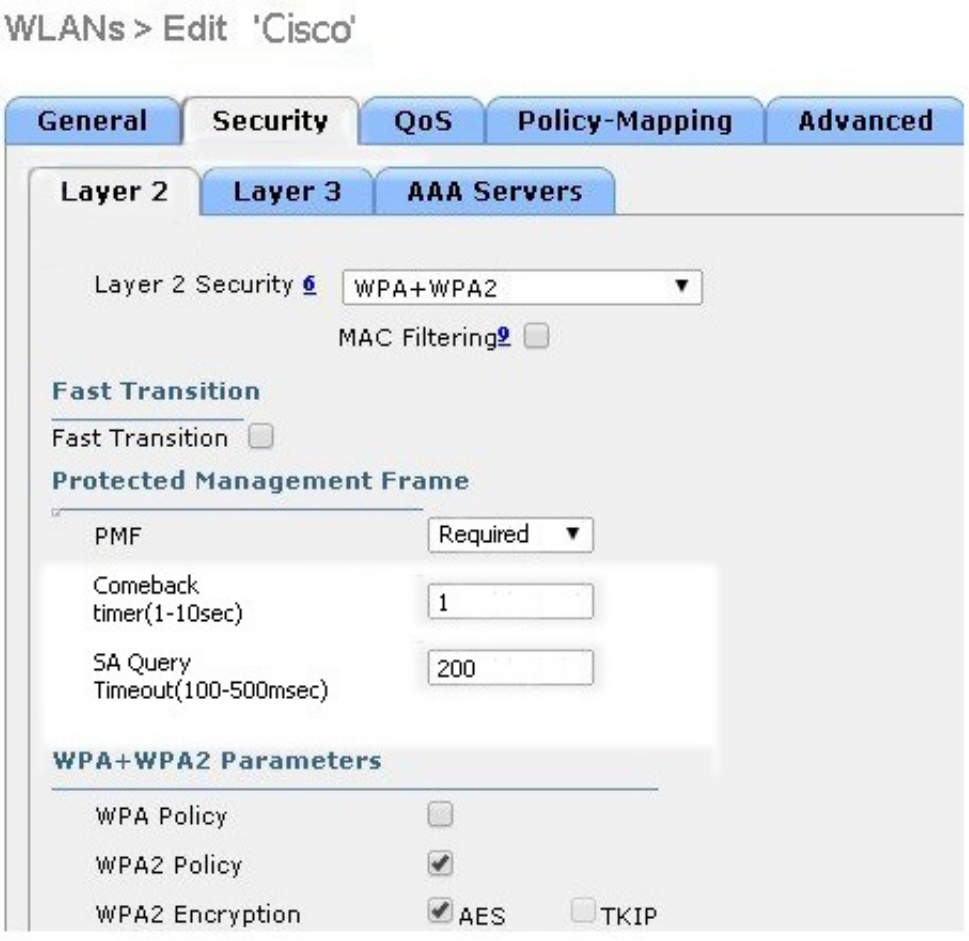
NEW QUESTION 15
An engineer has determined that the source of an authentication issue is the client laptop. Which three items must be verified for EAP-TLS authentication? (Choose three.)

A. The client certificate is formatted as X 509 version 3
B. The validate server certificate option is disabled.
C. The client certificate has a valid expiration date.
D. The user account is the same in the certificate.
E. The supplicant is configured correctly.
F. The subject key identifier is configured correctl

Answer: ADF

Explanation:

NEW QUESTION 16
Refer to the exhibit.



A customer is having problems with clients associating to me wireless network. Based on the configuration, which option describes the most likely cause of the issue?

A. Both AES and TKIP must be enabled
B. SA Query Timeout is set too low
C. Comeback timer is set too low
D. PME is set to "required"
E. MAC Filtering must be enabled

Answer: E

Explanation:

NEW QUESTION 18

MFP is enabled globally on a WLAN with default settings on single controller wireless network. Older client devices are disconnected from the network during a deauthentication attack. What is the
cause of this issue?

A. The client devices do not support WPA.
B. The client devices do not support CCXv5.
C. The MFP on the WLAN is set to optional
D. The NTP server is not configured on the controlle

Answer: C

Explanation:

NEW QUESTION 23
An engineer must enable EAP on a new WLAN and is ensuring that the necessary components are available. Which component uses EAP and 802.1x to pass user authentication to the authenticator?

A. AP
B. AAA server
C. supplicant
D. controller

Answer: D

Explanation:

NEW QUESTION 26
An engineer must provide a graphical trending report of the total number of wireless clients on the network. Winch report provides the required data?

A. Client Summary
B. Posture Status Count
C. Client Traffic Stream Metrics
D. Mobility Client Summary

Answer: D

Explanation:

NEW QUESTION 30
Which customizable security report on Cisco Prime Infrastructure would show rogue APs detected since a point in time?

A. New Rogue APs
B. Rogue AP Events
C. Rogue APs
D. Rogue AP Count Summary
E. Network Summary

Answer: C

Explanation:

NEW QUESTION 32
A customer is concerned that radar is impacting the access point that service the wireless network in an office located near an airport. On which type of channel should you conduct spectrum analysis to identify if radar is impacting the wireless network?

A. UNII-3 channels
B. UNII-1 channels
C. 802.11b channels
D. 2.4 GHz channels
E. UMII-2 channels
F. Channels 1, 5, 9, 13

Answer: E

Explanation:

NEW QUESTION 35
An engineer configures the wireless LAN controller to perform 802.1x user authentication. Which option must be enabled to ensure that client devices can connect to the wireless, even when WLC cannot communicate with the RADIUS?

A. local EAP
B. authentication caching
C. pre-authentication
D. Cisco Centralized Key Management

Answer: A

Explanation:

NEW QUESTION 36
A network engineer is implementing a wireless network and is considering deploying a single SSID for device onboarding. Winch option is a benefit of using dual SSIDs with a captive portal on the onboard SSID compared to a single SSID solution?

A. limit of a single device per user
B. restrict allowed devices types
C. allow multiple devices per user
D. minimize client configuration errors

Answer: B

Explanation:

NEW QUESTION 38
During the EAP process and specifically related to the logon session, which encrypted key is sent from the RADIUS server to the access point?

A. WPA key
B. encryption key
C. session key
D. shared secret key

Answer: C

Explanation:

NEW QUESTION 43
An engineer is deploying EAP-TLS as the authentication mechanism for an 802.1X-enabled wireless network. Which network device is responsible for applying the digital signature to a certificate to ensure that the certificate is trusted and valid?

A. supplicant
B. CA server
C. wireless controller
D. authentication server

Answer: B

Explanation:

NEW QUESTION 48
Which EAP type requires the use of device certificates?

A. EAP-TLS
B. EAP-FAST
C. EAP-SSL
D. PEAP
E. LEAP

Answer: A

Explanation:

NEW QUESTION 50
When a supplicant and AAA server are configured to use PEAP, which mechanism is used by the client to authenticate the AAA server in Phase One?

A. PMK
B. shared secret keys
C. digital certificate
D. PAC

Answer: C

Explanation:

NEW QUESTION 51
Which EAP types are supported by MAC 10.7 for authentication to a Cisco Unified Wireless Network?

A. LEAP and EAP-Fast only
B. EAP-TLS and PEAP only
C. LEAP, EAP-TLS, and PEAP only
D. LEAP, EAP-FAST, EAP-TLS, and PEAP

Answer: D

Explanation:

NEW QUESTION 56
What are two of the benefits that the Cisco AnyConnect v3.0 provides to the administrator for client WLAN security configuration? (Choose two.)

A. Provides a reporting mechanism for rouge APs
B. Prevents a user from adding any WLANs
C. Hides the complexity of 802.1X and EAP configuration
D. Supports centralized or distributed client architectures
E. Provides concurrent wired and wireless connectivity
F. Allows users to modify but not delete admin-created profiles

Answer: CD

Explanation:

NEW QUESTION 58
Clients are failing EAP authentication. A debug shows that an EAPOL start is sent and the clients are then de-authenticated. Which two issues can cause this problem? (Choose two.)

A. The WLC certificate has changed.
B. The WLAN is not configured for the correct EAP supplicant type.
C. The shared secret of the WLC and RADIUS server do not match.
D. The WLC has not been added to the RADIUS server as a client.
E. The clients are configured for machine authentication, but the RADIUS server is configured for user authentication.

Answer: CD

Explanation:

NEW QUESTION 60
Which feature should an engineer select to implement the use of VLAN tagging, QoS, and ACLs to clients based on RADIUS attributes?

A. per-WLAN RADIUS source support
B. client profiling
C. AAA override
D. captive bypassing
E. identity-based networking

Answer: C

Explanation:

NEW QUESTION 61
An engineer is implementing SNMP v3 on a wireless LAN controller and wants to use the combination of authentication and privacy protocols with the highest security available. Which protocols must be configured?

A. CFB-AES-128 with HMAC-MD5
B. CBC-DES with HMAC SHA
C. CFB-AES-128 with HMAC-SHA
D. CBC-DES with HMAC-MD5

Answer: C

Explanation:

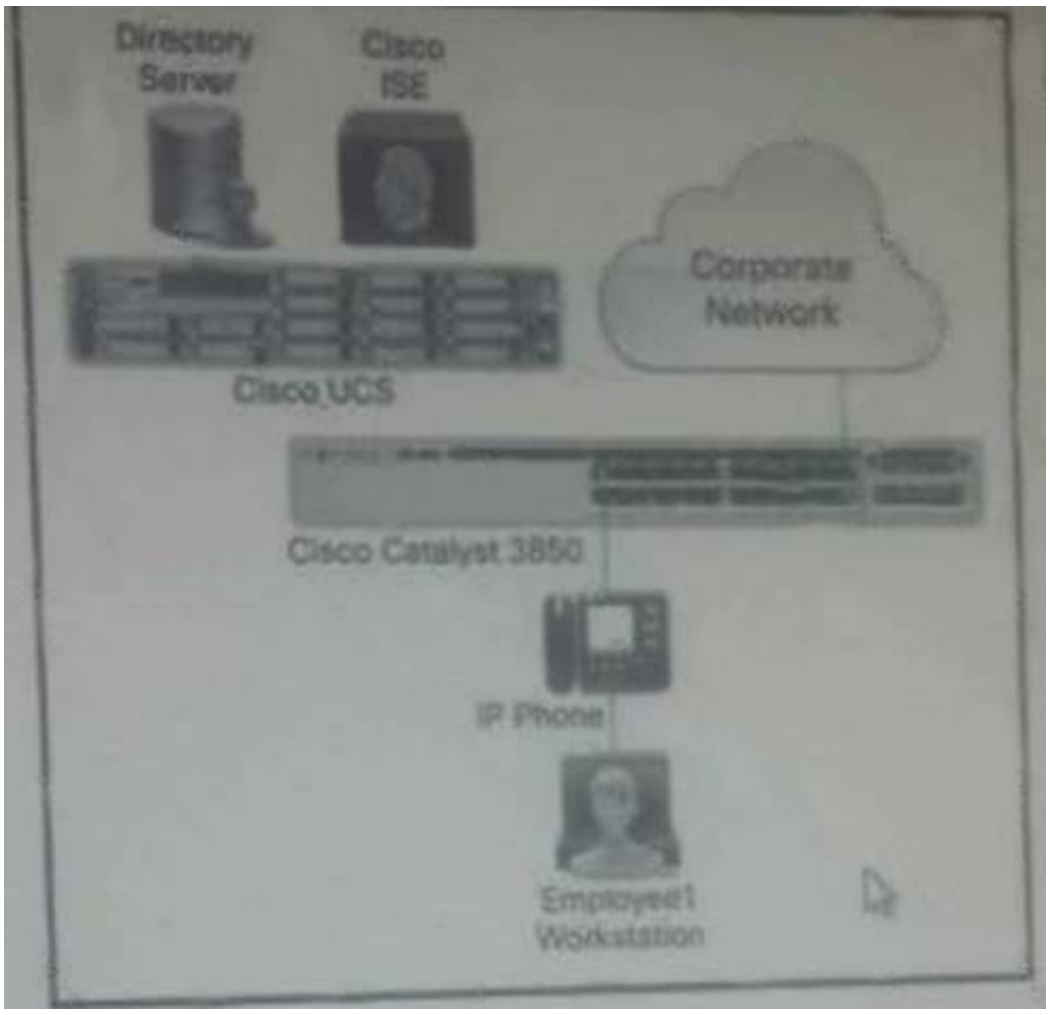
NEW QUESTION 62
Which three properties are used for client profiling of wireless clients? (Choose Three)

A. MAC OUI
B. IP Address
C. HTTP user agent
D. DHCP
E. hostname
F. OS Version

Answer: ACD

Explanation:

NEW QUESTION 63
Refer to the exhibit.



In this IBN topology, which device acts as the RADIUS server?

A. directory server
B. Cisco ISE
C. Cisco UCS
D. Cisco Catalyst 3850 Series Switch

Answer: D

Explanation:

NEW QUESTION 64
An engineer is configuring central web authentication using a Cisco 5508 wireless controller and the Cisco identity Service Engine. Which two attributes must be configured on Cisco ISE to add the controller as a network device? (Choose two.)

A. authentication protocol
B. RADIUS shared secret
C. out-of-band SGA PAC
D. controller IP address
E. controller software version

Answer: DE

Explanation:

NEW QUESTION 68
A company is deploying wireless PCs on forklifts within its new 10,000-square-foot (3048-squaremeter) facility. The clients are configured for PEAP-MS-CHAPv2 with WPA TKIP. Users report that applications frequently drop when the clients roam between access points on the floor. A professional site survey was completed. Which configuration change is recommended to improve the speed of client roaming?

A. EAP-FAST
B. EAP-TLS
C. WPA AES
D. WPA2 AES

Answer: D

Explanation:
Although the controller and APs support WLAN with SSID using WiFi Protected Access (WPA) and WPA2 simultaneously, it is common that some wireless client drivers cannot handle complex SSID settings. Whenever possible, Cisco recommends WPA2 only with Advanced Encryption Standard (AES). However, due to standards and mandatory WiFi Alliance certification process, TKIP support is required across future software versions. Keep the security policies simple for any SSID. Use a separate WLAN/SSID with WPA and Temporal Key Integrity Protocol (TKIP), and a separate one with WPA2 and Advanced Encryption Standard (AES). Since TKIP is being deprecated, Cisco recommends to use TKIP together with WEP, or to migrate out of TKIP completely and use PEAP, if possible.

NEW QUESTION 70
An engineer is troubleshooting rogue access points that are showing up in Cisco Prime Infrastructure. What is the maximum number of Aps the engineer can use to contain an identified rogue access point in the WLC?

A. 3
B. 4

C. 6
D. 5

Answer: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010 111001.html

NEW QUESTION 74
Which two statements describe the requirements for EAP-TLS?

A. It requires client-side and server-side certificates.
B. It uses PAC on the client.
C. It requires PKI.
D. It requires a server side digital certificate on only the RADIUS server
E. It must use AES for encryption and cannot use TKIP for encryptio

Answer: AB

Explanation:

NEW QUESTION 75
A customer wants the access points in the CEO's office to have different usernames and passwords for administrative support than the other access points deployed throughout the facility. Which feature can be enabled on the WLC and access points to achieve this criteria?

A. Override global credentials
B. HTTPS access
C. 802.1x supplicant credentials
D. local management users

Answer: D

Explanation:
You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information. This section provides instructions for initial configuration and for password recovery.
You can also set administrator usernames and passwords to manage and configure one or more access points that are associated with the switch. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-1/configuration_guide/b_161_consolidated_3650_cg/b_161_consolidated_3650_cg_chapter_01010 111.pdf

NEW QUESTION 77
An engineer is preparing to implement a BYOD SSID at remote offices using local switching and wants to ensure that Wi-Fi Direct clients can communicate after the SSID is deployed. The engineer is planning on implementing the config wlan wifidirect allow 1 command. Which Wi-Fi Direct Client Policy consideration is applicable?

A. Policy is applicable only with central switched WLANs on FlexConnect Aps.
B. Policy is applicable only when P2P is set to disabled.
C. Policy is applicable only to APs in FlexConnect mode only.
D. Policy is applicable only on WLANs that have APs in local mode onl

Answer: A

Explanation:

NEW QUESTION 80
WPA2 Enterprise with 802.1x is being used for clients to authenticate to a wireless network through an ISE server. For security reasons, the network engineer wants to ensure only PEAP authentication can be used. The engineer sent instructions to clients on how to configure their supplicants, but
users are still in the ISE logs authentication using EAP-FAST. Which option describes the most efficient way the engineer can ensure these users cannot access the network unless the correct
authentication mechanism is configured?

A. Enable AAA override on the SSID, gather the usernames of these users, and disable their RADIUS accounts until they make sure they correctly configured their devices.
B. Enable AAA override on the SSID and configure an access policy in ACS that denies access to the list of MACs that have used EAP-FAST.
C. Enable AAA override on the SSID and configure an access policy in ACS that allows access only when the EAP authentication method is PEAP.
D. Enable AAA override on the SSID and configure an access policy in ACS that puts clients that authenticated using EAP-FAST into a quarantine VLAN.

Answer: C

Explanation:

NEW QUESTION 84
A network engineer must segregate all iPads on the guest WLAN to a separate VLAN. How does the engineer accomplish this task without using ISE?

A. Use 802.1x authentication to profile the devices.

B. Create a local policy on the WLC.
C. Use an mDNS profile for the iPad device.
D. Enable RADIUS DHCP profiling on the WLAN.

Answer: B

Explanation:

NEW QUESTION 89
An engineer is configuring EAP-TLS with a client trusting server model and has configured a public root certification authority. Which action does this allow?

A. specifies a second certification authority to trust
B. utilizes two subcertification authority servers
C. creates a PKI infrastructure
D. validates the AAA server

Answer: D

Explanation:
To support EAP-TLS, the AAA server (for example, Cisco Secure ACS) must have a certificate. Either a public certification authority or a private certification authority can be used to issue the AAA server certificate. The AAA server will trust a client certificate that was issued from the same root certification authority that issued its certificate.
https://www.cisco.com/en/US/tech/ CK7 22/ CK8 09/technologies_white_paper09186a008009256b.sht ml

NEW QUESTION 92
An engineer is configuring a wireless network for local FlexConnect authentication. What three configurations are required for the WLC with WLAN 1 and AP Cisco? (Choose three.)

A. config ap filexconnect vlan enable Cisco
B. config wlan filexconnect vlan-central-switching 1 enable
C. config ap filexconnect vlan wlan 1 Cisco
D. config wlan filexconnect local-switching 1 enable
E. config wlan filexconnect ap-auth 1 enable
F. config ap mode filexconnect Cisco

Answer: ACD

Explanation:

NEW QUESTION 97
While deploying PEAP authentication on a customer laptop with the native Windows supplicant, the PEAP security options do not appear. Which option describes what must be done?

A. Enable automatic connection to the WLAN.
B. Enable static DNS on the WLAN.
C. Enable AES on the WLAN settings.
D. Enable WLAN autoconfig services on the P

Answer: C

Explanation:

NEW QUESTION 98
A wireless engineer wants to view how many wIPS alerts have been detected in Cisco Prime. Which tab does the engineer select in the wireless dashboard?

A. Security
B. Cleanair
C. Context Aware
D. Mesh

Answer: A

Explanation:

NEW QUESTION 101
You are configuring the social login for a guest network. Which three options are configurable social connect in Cisco CMS visitor connect? (Choose three.)

A. Linkedin
B. Pinterest
C. Medium
D. Google+
E. Facebook
F. MySpace

Answer: ADE

Explanation:

NEW QUESTION 105
Which three methods are valid for guest wireless using web authentication? (Choose three.)

A. LDAP
B. SSL
C. local
D. TLS
E. EAP-TLS
F. RADIUS

Answer: ACF

Explanation:
There are three ways to authenticate users when you use web authentication. Local authentication allows you to authenticate the user in the Cisco WLC. You can also use an external RADIUS server or a LDAP server as a backend database in order to authenticate the users.
https://www.sslshopper.com/ssl-certificate-not-trusted-error.html

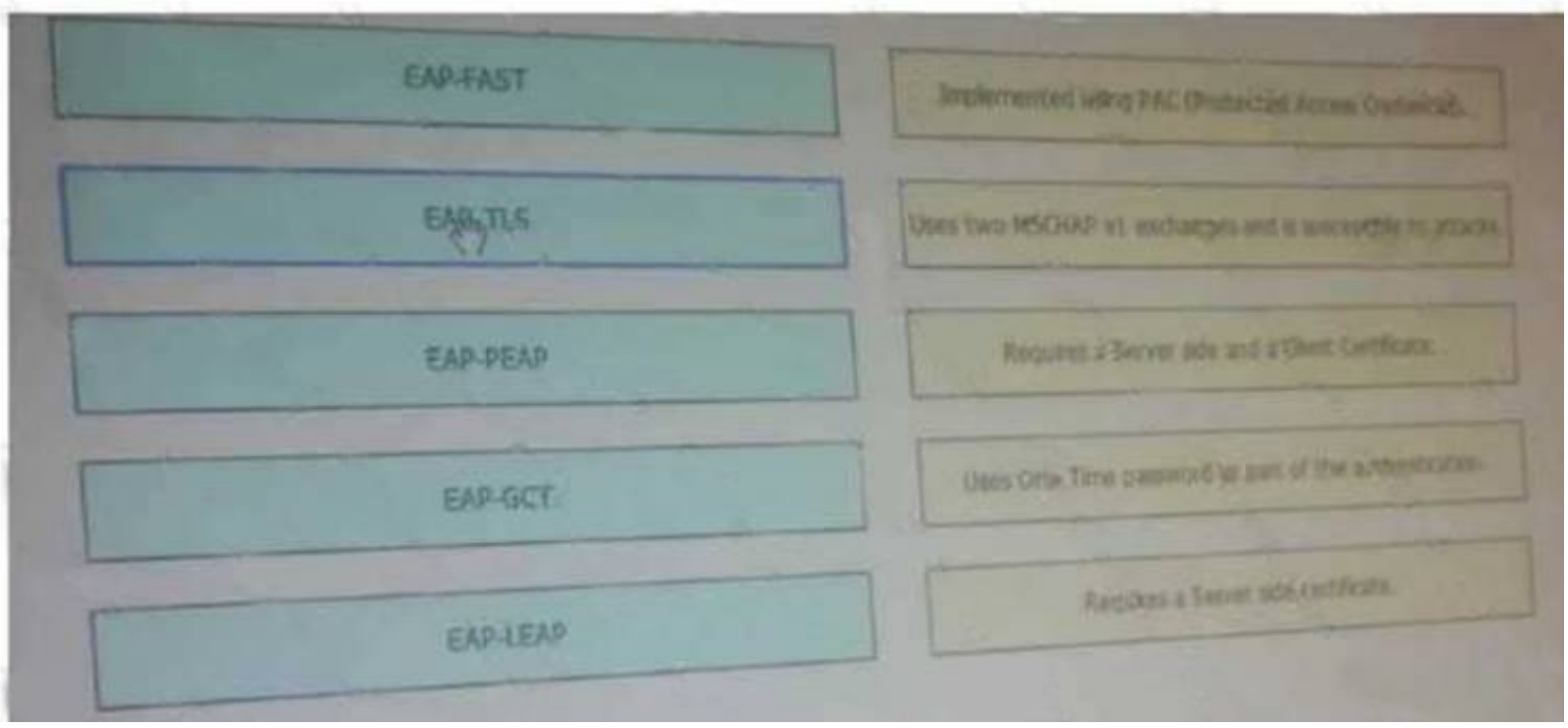
NEW QUESTION 109
When implementing secure PCI wireless networks, which two are specific recommendations in the PCI DSS? (Choose two)

A. Use a minimum 12-character random passphrase with WPA
B. Segment logging events with other networking devices within the organization.
C. Use VLAN based segmentation with MAC filters.
D. Change default settings.
E. Implement strong wireless authentication

Answer: DE

Explanation:
Wireless networks that are part of the CDE must comply with all PCI DSS requirements. This includes using a firewall (requirement 1.2.3) and making sure that additional rogue wireless devices have not been added to the CDE (requirement 11.1). In addition, PCI DSS compliance for systems that include WLANs as a part of the CDE requires extra attention to WLAN specific technologies and processes such as:
A. Physical security of wireless devices, B. Changing default passwords and settings on wireless devices, C. Logging of wireless access and intrusion prevention, D. Strong wireless authentication and encryption, E. Use of strong cryptography and security protocols, and F. Development and enforcement of wireless usage policies. This section will cover each of these requirements sequentially. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

NEW QUESTION 114
DRAG DROP
Drag the EAP Authentication type on the left to the accurate description provided on the right



Answer:

Explanation:

eap-fast	implemented using pac
eap-tls	requeires a server side certificate
eap-peap	uses one time password as part of the authentication
eap-leap	requires a server side and a client certificate
eap-gct	uses two MSCHAP v1 exchanges and is susceptible to attcks

NEW QUESTION 115
Refer to the exhibit.

```
(Test-1) >show network summary
RF-Network Name. . . . . . . . . . . . . . . . . . . . . . Test-1
Web Mode. . . . . . . . . . . . . . . . . . . . . . . . . . Disable
Secure Web Mode. . . . . . . . . . . . . . . . . . . . . . Enable
Secure Web Mode Cipher-Option High. . . . . . . . . . . . .Disable
Secure Web Mode Cipher-Option SSLv2. . . . . . . . . . . . Disable
Secure Web Mode RC4 Cipher Preference. . . . . . . . . . . Disable
OCSP. . . . . . . . . . . . . . . . . . . . . . . . . . . .  Disabled
OSCP responder URL. . . . . . . . . . . . . . . . . . . . .
Secure Shell (ssh) . . . . . . . . . . . . . . . . . . . . Enable
Telnet. . . . . . . . . . . . . . . . . . . . . . . . . . . .Disable
Ethernet Multicast Forwarding. . . . . . . . . . . . . . . Disable
Ethernet Broadcast Forwarding. . . . . . . . . . . . . . . Disable
IPv4 AP Multicast/Broadcast Mode. . . . . . . . . . . . . .Unicast
IGMP snooping . . . . . . . . . . . . . . . . . . . . . . . .Disabled
IGMP timeout. . . . . . .. . . . . . . . . . . . . . . . . . 60 seconds
IGMP Query Interval. . . . . . . . . . . . . . . . . . . . . 20 seconds
MLD snooping. . . . . . . . . . . . . . . . . . . . . . . . .Disabled
MLD timeout. . . . . . . . . . . . . . . . . . . . . . . . . 60 seconds
MLD query interval. . . . . . . . . . . . . . . . . . . . . .20 seconds
User Idle Timeout. . . . . . . . . . . . . . . . . . . . . . 3600 seconds
ARP Idle Timeout. . . . . . . . . . . . . . . . . . . . . . .3600 seconds
Cisco Join Priority. . . . . . . . . . . . . . . . . . . . ..Disable
AP Join Priority. . . . . . . . . . . . . . . . . . . . . . .Disable
_
WebPortal Online Client. . . . . . . . . . . . . . . . . . . 0
mDNS snooping. . . . . . . . . . . . . . . . . . . . . . . . Disabled
mDNS Query Interval. . . . . . . . . . . . . . . . . . . . . 15 minutes

(Test-1) >show mdns service summary
Number of Services. . . . . . . . . . . . . . . . . . . . . 5

Service-name                    LSS    Origin    No SP  Service-string
------------------------------  ----   --------- -----  ------------------
AirPrint                         No     All        0    _ipp._tcp.local.
AppleTV                          No     All        0    _airplay._tcp.local.
HP_Photosmart_Printer_1          No     All        0    _universal._sub._ipp.
_tcp.local.
HP_Photosmart_Printer_2          No     All        0    _cups._sub._ipp._tcp.
local.
Printer                          No     All        0    _printer._tcp.local
```

An engineer has configured a BYOD policy that allows for printing on the WLAN utilizing Bonjour services. However, the engineer cannot get printing working. The WLC firmware is 8.x. the printer is connected on the wired network where a few of the access points are also connected.
Which reason that printing is not working is true?

A. Location-specific service is not enabled on the WLC.
B. Secure Web Mode Cipher-Option SSLv2 is not enabled.
C. mBNS and IGMP snooping is not enabled on the WLC.
D. IGMP Query Interval value is too low.
E. The number of mDNS services exceeds firmware limits.

Answer: A

Explanation:

NEW QUESTION 118
Which two fast roaming algorithms will allow a WLAN client to roam to a new AP and re-establish a new session key without a full reauthentication of the WLAN client? (Choose two.)

A. PKC
B. GTK
C. PMK
D. PTK
E. CKM

Answer: AE

Explanation:

NEW QUESTION 121
Which condition introduce security risk to a BYOD policy?

A. enterprise-managed MDM platform used for personal devices
B. access to LAN without implementing MDM solution
C. enforcement of BYOD access to internet only network
D. enterprise life-cycle enforcement of personal device refresh

Answer: B

Explanation:

NEW QUESTION 123
An engineer ran the PCI report in Cisco Prime Infrastructure and received a warning on PCIDSS
Requirement 2.1.1 that the SNMP strings are set to default and must be changed. Which tab in the Cisco WLC can the engineer use to navigate to these settings?

A. Management
B. Security
C. Controller
D. Wireless

Answer: A

Explanation:

NEW QUESTION 128
Refer to the exhibit.

```
wlan CORP_BYOD 1 CORP_BYOD
client vlan 30
nac
ip dhcp required
session-timeout 86400
no shutdown
```

A network engineer must configure a WLAN on a Cisco IOS-XE controller to support corporate devices (using VLAN 30) and BYOD (using VLAN 40) on the same secure SSID. The security team has built an ISE deployment to be used for VLAN assignment and to restrict access based on policy and posture compliance.
Given the existing WLAN configuration, which configuration change must be made?

A. remove ip dhcp required
B. Add aaa-override
C. Remove nac
D. Add mac-filtering default

Answer: B

Explanation:

NEW QUESTION 131
Which EAP method can an AP use to authenticate to the wired network?

A. EAP-GTC
B. EAP-MD5
C. EAP-TLS
D. EAP-FAST

Answer: C

Explanation:

NEW QUESTION 132
An engineer with ID 338860948 is implementing Cisco Identity-Based Networking on a Cisco AireOS
controller. The engineer has two ACLs on the controller. The first ACL, named BASE_ACL, is applied to the corporate_clients interface on the WLC, which is used for all corporate clients. The second ACL, named HR_ACL, is referenced by ISE in the Human Resources group policy.
Which option is the resulting ACL when a Human Resources user connects?

A. HR_ACL only
B. HR_ACL appended with BASE_ACL
C. BASE_ACL appended with HR_ACL
D. BASE_ACL only

Answer: A

Explanation:

NEW QUESTION 136
Refer to the exhibit.

```
(Cisco Controller) >show radius summary
Authentication Servers
Idx Type Server Address Port State Tout MgmtTout RFC3576
--- ---- --------------- ------ -------- ---- -------- ---------
1 N 10.10.2.3 1812 Enabled 2 2 Enabled
2 N 10.10.2.4 1812 Enabled 2 2 Enabled

Accounting Servers
Idx Type Server Address Port State Tout MgmtTout RFC3576
--- ---- --------------- ------- ------- ---- -------- ---------
1 N 10.10.2.3 1813 Enabled 2 2 N/A
2 N 10.10.2.4 1813 Enabled 2 2 N/A
```

An engineer utilizing ISE as the wireless AAA service noticed that the accounting process on the server at 10.10.2.3 has failed, but authentication process is still functional.
Which ISE nodes receive WLC RADIUS traffic, using the CLI output and assuming the WLAN uses the servers in their indexed order?

A. authentication to 10.10.2.4, accounting to 10.10.2.3.
B. authentication to 10.10.2.3, accounting to 10.10.2.3.
C. authentication to 10.10.2.4, accounting to 10.10.2.4.
D. authentication to 10.10.2.3, accounting to 10.10.2.4.

Answer: B

Explanation:

NEW QUESTION 141
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-375 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-375-dumps.html