C. End-user training manuals for the policies to be created.
D. Awareness of the exact vendor devices being installed.

Correct Answer: A

QUESTION 15
What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hotspots?

A. Require Port Address Translation (PAT) on each laptop.
B. Require secure applications such as POP, HTTP, and SSH.
C. Require VPN software for connectivity to the corporate network.
D. Require WPA2-Enterprise as the minimal WLAN security solution.

Correct Answer: C

QUESTION 16
What EAP type supports using MS-CHAPv2, EAP-GTC or EAP-TLS for wireless client authentication?

A. EAP-GTC
B. PEAP
C. EAP-TTLS
D. LEAP
E. H-REAP

Correct Answer: B

QUESTION 17
You must implement 7 APs for a branch office location in your organizations. All APs will be autonomous and provide the same two SSIDs (CORP1879 and Guest). Because each AP is managed directly through a web-based interface, what must be changed on every AP before enabling the WLANs to ensure proper staging procedures are followed?

A. Output power
B. Fragmentation threshold
C. Administrative password
D. Cell radius

Correct Answer: C

QUESTION 18
You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet. What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

A. Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.
B. Use internal antennas.
C. Use external antennas.

D.   Power the APs using PoE.

Correct Answer: A

QUESTION 19
Fred works primarily from home and public wireless hotspots rather than commuting to office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN. In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

A.   Use enterprise WIPS on the corporate office network.
B.   Use 802.1X/PEAPv0 to connect to the corporate office network from public hotspots.
C.   Use secure protocols, such as FTP, for remote file transfers.
D.   Use an IPSec VPN for connectivity to the office network.
E.   Use only HTTPS when agreeing to acceptable use terms on public networks.
F.   Use WIPS sensor software on the laptop to monitor for risks and attacks.

Correct Answer: D

QUESTION 20
Which one of the following is not a role defined in the 802.1X authentication procedures used in 802.11 and 802.3 networks for port-based authentication?

A.   AAA Server
B.   Authentication Server
C.   Supplicant
D.   Authenticator

Correct Answer: A

QUESTION 21
What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

A.   RC5 stream cipher
B.   Block cipher support
C.   Sequence counters
D.   32-bit ICV (CRC-32)
E.   Michael

Correct Answer: E

QUESTION 22
Which of the following is a valid reason to avoid the use of EAP-MD5 in production WLANs?

A.   It does not support a RADIUS server.
B.   It is not a valid EAP type.
C.   It does not support mutual authentication.
D.   It does not support the outer identity.

Correct Answer: C

QUESTION 23
Your organization is using EAP as an authentication framework with a specific type that meets the requirements of your corporate policies. Which one of the following statements is true related to this implementation?

A. The client STAs may communicate over the controlled port in order to authenticate as soon as the Open System authentication completes.
B. The client STAs may communicate over the uncontrolled port in order to authenticate as soon as the Open System authentication completes.
C. The client STAs may use a different, but complementary, EAP type than the AP STAs.
D. The client will be the authenticator in this scenario.

Correct Answer: B

QUESTION 24
A WLAN consultant has just finished installing a WLAN controller with 15 controller-based APs. Two SSIDs with separate VLANs are configured for this network, and both VLANs are configured to use the same RADIUS server. The SSIDs are configured as follows:

▪ SSID Blue -VLAN 10 -Lightweight EAP (LEAP) authentication -CCMP cipher suite
▪ SSID Red -VLAN 20 -PEAPv0/EAP-TLS authentication -TKIP cipher suite

The consultant's computer can successfully authenticate and browse the Internet when using the Blue SSID. The same computer cannot authenticate when using the Red SSID. What is a possible cause of the problem?

A. The consultant does not have a valid Kerberos ID on the Blue VLAN.
B. The client does not have a proper certificate installed for the tunneled authentication within the established TLS tunnel.
C. The TKIP cipher suite is not a valid option for PEAPv0 authentication.
D. The Red VLAN does not use server certificate, but the client requires one.

Correct Answer: B

QUESTION 25
Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM. What device functions as the 802.1X/EAP Authenticator?

A. WLAN Controller/AP
B. MacBook Pro
C. SRV21
D. RADIUS server

Correct Answer: A

QUESTION 26
In an IEEE 802.11-compliant WLAN, when is the 802.1X Controlled Port placed into the unblocked state?

A. After EAP authentication is successful
B. After Open System authentication
C. After the 4-Way Handshake
D. After any Group Handshake

Correct Answer: A

QUESTION 27
When using a tunneled EAP type, such as PEAP, what component is protected inside the TLS tunnel so that it is not sent in clear text across the wireless medium?

A. Server credentials
B. User credentials
C. RADIUS shared secret
D. X.509 certificates

Correct Answer: B

QUESTION 28
What protocol, listed here, allows a network manager to securely administer the network?

A. TFTP
B. Telnet
C. HTTPS
D. SNMPv2

Correct Answer: C

QUESTION 29
XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization. What RADIUS feature could be used by XYZ to assign the proper network permissions to users during authentications?

A. RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to-SSID mapping table in the LDAP user database.
B. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.
C. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
D. RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.

Correct Answer: B

QUESTION 30
Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

A. Provide two or more user groups connected to the same SSID with different levels of network privileges.

B.   Allow access to specific files and applications based on the user's WMM access category.
C.   Allow simultaneous support for multiple EAP types on a single access point.
D.   Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.

Correct Answer: A

QUESTION 31
A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication. For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

A.   SNMPv3 support
B.   802.1Q VLAN trunking
C.   Internal RADIUS server
D.   WIPS support and integration
E.   WPA2-Enterprise authentication/encryption

Correct Answer: C

QUESTION 32
ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC's preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources. What security best practices should be followed in this deployment scenario?

A.   Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.
B.   RADIUS services should be provided at branch offices so that authentication server and suppliant credentials are not sent over the Internet.
C.   An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
D.   APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.

Correct Answer: C

QUESTION 33
ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication. How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2-Enterprise WLAN security solution?

A.   Implement a RADIUS server and query user authentication requests through the LDAP server.
B.   Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily