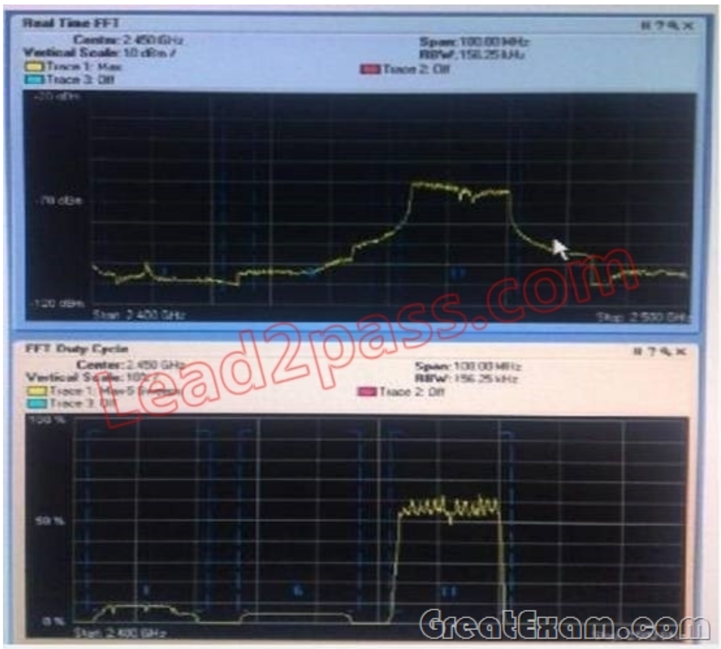
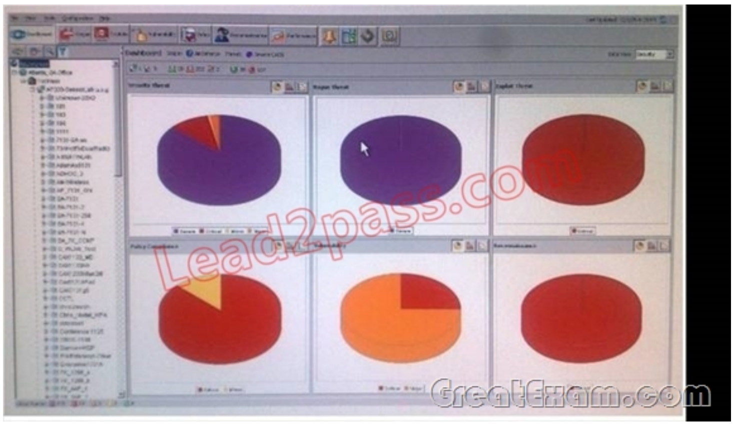
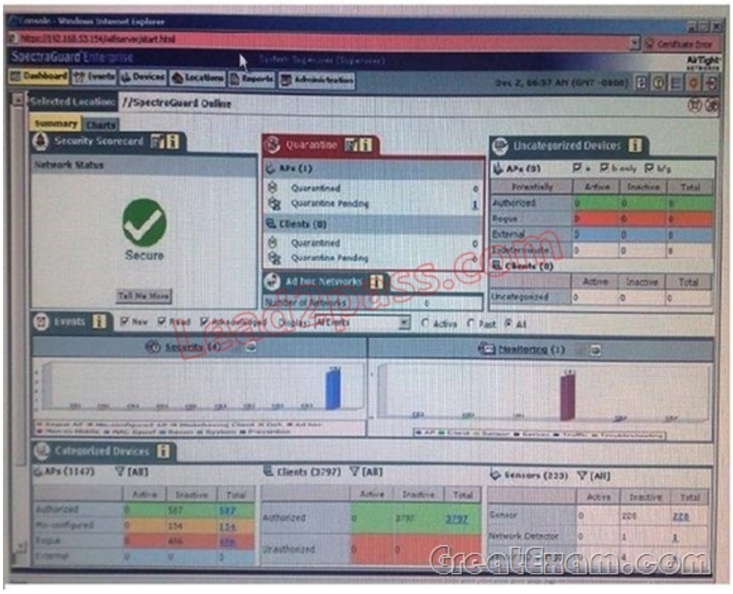
Free Download Pass4sure and Lead2pass CWNP PW0-204 Exam Question with PDF & VCE (11-20)

QUESTION 11The IEEE 802.11 pairwise transient key (PTK) is derived from what cryptographic element?A. Phase shift key (PSK)B. Group master key (GMK)C. Peerkey (PK)D. Group temporal key (GTK)E. Pairwise master key (PMK) Answer: E QUESTION 12What wireless authentication technologies build a TLS-encrypted tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3) A. EAP-TTLSB. EAP-FASTC. LEAPD. EAP-MD5E. MS-CHAPv2F. PEAPv1/EAP-GTC Answer: ABF QUESTION 13Given:ABC Company has recently installed a WLAN controller and configured it to support WPA2- Enterprise security. The administrator has confirmed a security profile on the WLAN controller for each group within the company (manufacturing, sales, and engineering) How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller? A. The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication. B. The RADIUS server forwards a request for a group attribute to an LDAP database service, and LDAP sends the group attribute to the WLAN controller.C. The RADIUS server sends a group name return list attribute to the WLAN controller during every successful user authentication.D. The RADIUS server sends the list of authenticated users and groups to the WLAN controller as a part of a 4-way handshake prior to user authentication. Answer: B QUESTION 14Given:Jane Smith works primarily from home and public wireless hot spot rather than commuting to the office. She frequently accesses the office network frequently from her laptop using the 802.11 WLAN.To safeguard her data, what wireless security policy items should be implemented? (Choose 2) A. Use 802.1X/PEAPv0 to connect to the corporate office network.B. Use secure protocols, such as FTP, for remote file transfer with encryption.C. Use an IPSec VPN for connectivity to the office network.D. Use an HTTPS captive portal for authent6ication at hot spots.E. Use WIPS sensor software to monitor for risks.F. Use personal firewall software on her laptop. Answer: CF QUESTION 15What is illustrated on the RF spectrum analyzer?



A. A low-power narrow band RF attacks is in progress on channel 11, causing significant 802.11 interference.B. A frequency hoping device is being used as a signal jammer on channel 11 only.C. An HR/DSSS AP and an ERP AP are both operating on channel 11 simultaneously.D. An ERP AP operating normally on channel 11. Answer: A QUESTION 16What security weakness is presented in pre-RSNA system using 802.1X with dynamic WEP? A. There is support for authentication of individual users.B. All version of EAP used with dynamic WEP pass the user name across the wireless medium in clear text.C. The session key is crackable if enough traffic is transmitted using the key.D. With out notification, APs downgrade the security mechanism to 104-bit static WEP when the client device does not support dynamic WEP. Answer: C QUESTION 17In what deployment scenarios would it be desirable to enable peer-to-peer traffic blocking? A. In home networks in which file and pointer sharing is enabledB. In corporate VoWiFi is networks with push to talk multicast capabilitiesC. At public hotspots in which many clients use diverse applicationD. In university environment with multicast training Answer: C QUESTION 18What type of system is installed in graphics?





Quarantine

APs (1)
Quarantined 0
Quarantine Pending 1

Clients (0)
Quarantined 0
Quarantine Pending 0

Ad hoc Networks
Number of Networks 0

Uncategorized Devices — APs (0)

Potentially	Active	Inactive	Total
Authorized	0	0	0
Rogue	0	0	0
External	0	0	0
Indeterminate	0	0	0

Clients (0)

	Active	Inactive	Total
Uncategorized	0	0	0

Categorized Devices

APs (1147) [All]

	Active	Inactive	Total
Authorized	0	587	587
Mis-configured	0	154	154
Rogue	0	406	406
External	0	0	0

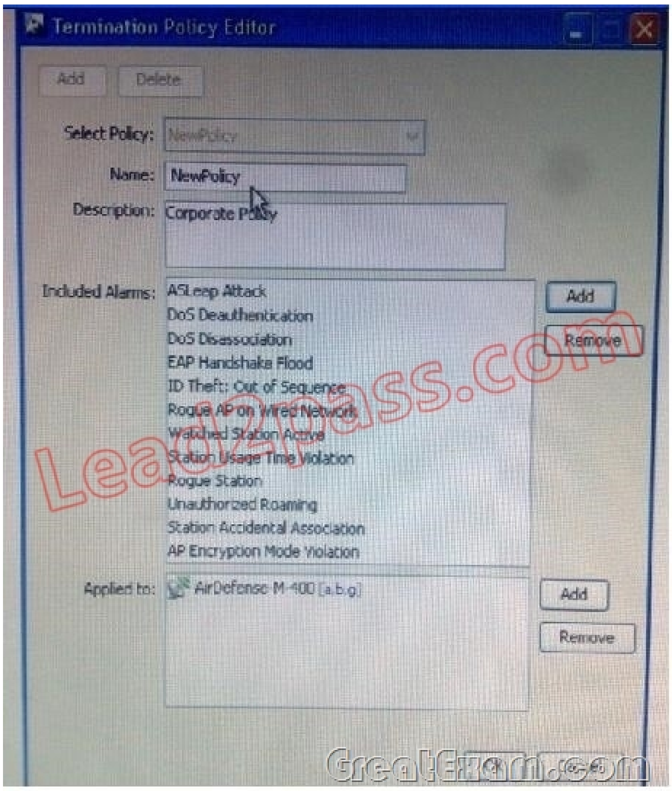
Clients (3797) [All]

	Active	Inactive	Total
Authorized	0	3797	3797
Unauthorized	0	0	

Sensors (223) [All]

	Active	Inactive	Total
Sensor	0	222	222
Network Detector	0	1	1

A. Distributed RF spectrum analyzerB. Wireless Intrusion Prevention SystemC. WLAN Controller Device MonitorsD. WLAN Emulation SystemE. Wireless VPN Management System Answer: B QUESTION 19Given:Many corporations have guest VLANs configured on their WLAN controller that allow visitors to have wireless internet access only.What risks are associated with implementing the guest VLAN without any protocol filtering features enabled? (Choose 2) A. Unauthorized users can perform internet based network attacks through the WLAN.B. Intruders can send spam to the internet through the guest VLAN.C. Peer-to-peer attacks between the guest users can not be prevented without protocol filtering.D. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.E. Guest users can reconfigure APs in the guest VKAN unless unsecure network management protocols (e.g. Telnet, HTTP) are filtered. Answer: AC QUESTION 20Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAPPEAPv0. The company's wireless network action network administrator assured Joe that his laptop was authorized in the WIPS for connectivity to all marketing department APs before it was given to him yesterday the WIPS terminations given to him yesterday. The WIPS termination policy is shown in exhibit.Whatis apossible reason that Joe can not connect to the network?



Select Policy: NewPolicy

Name: NewPolicy

Description: Corporate Policy

Included Alarms: ASLeap Attack
DoS Deauthentication
DoS Disassociation
EAP Handshake Flood
ID Theft: Out of Sequence
Rogue AP on Wired Network
Watched Station Active
Station Usage Time Violation
Rogue Station
Unauthorized Roaming
Station Accidental Association
AP Encryption Mode Violation

Applied to: AirDefense M-400 [a,b,g]

A. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.B. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate.This WIPS responded by disabling the APs.C. Joe's 802.11radio sending too many probe request and EAPoL start frame due to corrupted driver.D. Joe configured his 802.11 radio card to transmit at 100mW to increase his SNR. The WIPS is detecting his much out put power as a DoS attack.E. Joe changed the system limit on his computer, and WIPS is detecting this as usage time violation. Answer: A If you want to pass the CWNP PW0-204 exam sucessfully, recommend to read latest CWNP PW0-204 Dumps full version.