This page was exported from - Braindump2go Exam Dumps Free Download
Export date: Thu Mar 28 21:32:50 2024 / +0000 GMT

[210-260 New VCE100% Real Exam Questions-Braindump2go 210-260 PDF and 210-260 VCE Dumps 265Q Download[91-100

(2017 June)Cisco 210-260 Exam Dumps with PDF and VCE New Updated in www.Braindump2go.com Today!100% Real Exam Questions! 100% Exam Pass Guaranteed!1.|2017 Version New 210-260 PDF and 210-260 VCE 265Q&As Download: http://www.braindump2go.com/210-260.html 2.|2017 Version New 210-260 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNV1RGaFJYZkxGWFk?usp=sharing QUESTION 91Which type of address translation should be used when a Cisco ASA is in transparent mode? A. Static NATB. Dynamic NATC. OverloadD. Dynamic PAT Answer: A QUESTION 92Which components does HMAC use to determine the authenticity and integrity of a message? (Choose two.) A. The passwordB. The hashC. The keyD. The transform set Answer: BC QUESTION 93What is the default timeout interval during which a router waits for responses from a TACACS server before declaring a timeout failure? A. 5 secondsB. 10 secondsC. 15 secondsD. 20 seconds Answer: AExplanation:Router(config)#tacacs-server timeout ?<1-1000> Wait time (default 5 seconds) QUESTION 94Which RADIUS server authentication protocols are supported on Cisco ASA firewalls? (Choose three.) A. EAPB. ASCIIC. PAPD. PEAPE. MS-CHAPv1F. MS-CHAPv2 Answer: CEFExplanation: The ASA supports the following authentication methods with RADIUS servers:PAP - For all connection types.CHAP and MS-CHAPv1 - For L2TP-over-IPsec connections.MS-CHAPv2 - For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections. Authentication Proxy modes - For RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS- to-Token server http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_radius.html#77318 QUESTION 95Which command initializes a lawful intercept view? A. username cisco1 view lawful-intercept password ciscoB. parser view cisco li-viewC. li-view cisco user cisco1 password ciscoD. parser view li-view inclusive Answer: CExplanation: Before you initialize a lawful intercept view, ensure that the privilege level is set to 15 via the privilege command.SUMMARY STEPS1. enable view2. configure terminal3. li-view li-password user username password password4. username lawful-intercept [name] [privilege privilege-level| view view-name] password password5. parser view view-name6. secret 5 encrypted-password7. name new-name QUESTION 96Which security measures can protect the control plane of a Cisco router? (Choose two.) A. CCPr B. Parser viewsC. Access control listsD. Port securityE. CoPP Answer: AEExplanation:Table 10-3 Three Ways to Secure the Control PlaneUsing CoPP or CPPr, you can specify which types of management traffic are acceptable at which levels.For example, you could decide and configure the router to believe that SSH is acceptable at 100 packets per second, syslog is acceptable at 200 packets per second, and so on. Traffic that exceeds the thresholds can be safely dropped if it is not from one of your specific management stations. You can specify all those details in the policy.You learn more about control plane security in Chapter 13, "Securing Routing Protocols and the Control Plane."Selective Packet Discard (SPD) provides the ability toAlthough not necessarily a security feature,prioritize certain types of packets (for example, routing protocol packets and Layer 2 keepalive messages, route processor [RP]). SPD provides priority of critical control plane traffic which are received by theover traffic that is less important or, worse yet, is being sent maliciously to starve the CPU of resources required for the RP. QUESTION 97Which statement about extended access lists is true? A. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the destinationB. Extended access lists perform filtering that is based on source and destination and are most effective when applied to the sourceC. Extended access lists perform filtering that is based on destination and are most effective when applied to the sourceD. Extended access lists perform filtering that is based on source and are most effective when applied to the destination Answer: BExplanation:Standard ACL1) Able Restrict, deny & filter packets by Host Ip or subnet only.2) Best Practice is put Std. ACL restriction near from Source Host/Subnet (Interface-In-bound).3) No Protocol based restriction. (Only HOST IP).Extended ACL1) More flexible then Standard ACL.2) You can filter packets by Host/Subnet as well as Protocol/TCPPort/UDPPort.3) Best Practice is put restriction near form Destination Host/Subnet. (Interface-Outbound) QUESTION 98Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.) A. FTPB. SSHC. TelnetD. AAAE. HTTPSF. HTTP Answer: BE QUESTION 99What are the primary attack methods of VLAN hopping? (Choose two.) A. VoIP hoppingB. Switch spoofingC. CAM-table overflowD. Double tagging Answer: BD QUESTION 100How can the administrator enable permanent client installation in a Cisco AnyConnect VPN firewall configuration? A. Issue the command anyconnect keep-installer under the group policy or username webvpn modeB. Issue the command anyconnect keep-installer installed in the global configurationC. Issue the command anyconnect keep-installer installed under the group policy or username webvpn modeD. Issue the command anyconnect keep-installer installer under the group policy or username webvpn mode Answer: C !!!RECOMMEND!!! 1.|2017 Version New 210-260 PDF and 210-260 VCE 265Q&As

Download:http://www.braindump2go.com/210-260.html 2.|2017 Version New 210-260 Study Guide Video: YouTube Video: YouTube.com/watch?v=9yy5IlptXYw