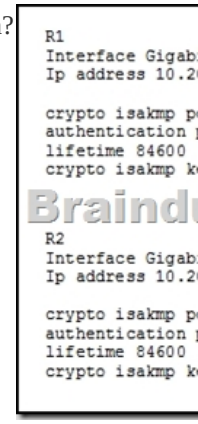
[2017-Oct.-New100% Real 210-260 PDF Questions and Answers 362Q-Braindump2go[136-150

2017 Oct New 210-260 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 210-250 Questions:
1.|2017 New 210-260 Exam Dumps (PDF & VCE) 362Q&As Download:https://www.braindump2go.com/210-260.html 2.|2017 New 210-260 Exam Questions & Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNV1RGaFJYZkxGWFk?usp=sharing QUESTION 136Which FirePOWER preprocessor engine is used to prevent SYN attacks? A. Anomaly.B. Rate-Based PreventionC. Portscan DetectionD. Inline Normalization Answer: B QUESTION 137What is the only permitted operation for processing multicast traffic on zone-based firewalls? A. Stateful inspection of multicast traffic is supported only for the self-zone.B. Stateful inspection of multicast traffic is supported only between the self-zone and the internal zone.C. Only control plane policing can protect the control plane against multicast traffic.D. Stateful inspection of multicast traffic is supported only for the internal zone Answer: CExplanation:Stateful inspection of multicast traffic is NOT supported by Cisco Zone based firewalls OR Cisco Classic firewall. QUESTION 138Which of encryption technology has the broadcast platform support to protect operating systems? A. MiddlewareB. HardwareC. software D. file-level Answer: C QUESTION 139Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attack? A. holistic understanding of threatsB. graymail management and filteringC. signature-based IPSD. contextual analysis Answer: D QUESTION 140Which Sourfire secure action should you choose if you want to block only malicious traffic from a particular end-user? A. TrustB. BlockC. Allow without inspectionD. MonitorE. Allow with inspection Answer: EExplanation:Allow with Inspection allows all traffic except for malicious traffic from a particular end-user. The other options are too restrictive, too permissive, or don't exist. QUESTION 141Which two next-generation encryption algorithms does Cisco recommends? (Choose two) A. SHA-384B. MD5C. DH-1024D. DESE. AESF. 3DES Answer: AE Explanation:From Cisco documentation:A. SHA-384 - YESB. MD5 - NOC. DH-1024 - NOD. DES - NOE. AES - YES (CBC, or GCM modes)F. 3DES - Legacy QUESTION 142When an administrator initiates a device wipe command from the ISE, what is the immediate effect? A. It requests the administrator to choose between erasing all device data or only managed corporate data.B. It requests the administrator to enter the device PIN or password before proceeding with the operationC. It immediately erases all data on the device.D. It notifies the device user and proceeds with the erase operation Answer: A QUESTION 143How does a device on a network using ISE receive its digital certificate during the new-device registration process? A. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA serverB. The device request a new certificate directly from a central CAC. ISE issues a pre-defined certificate from a local databaseD. ISE issues a certificate from its internal CA server. Answer: AExplanation:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf
QUESTION 144How can you detect a false negative on an IPS? A. View the alert on the IPSB. Use a third-party to audit the next-generation firewall rulesC. Review the IPS consoleD. Review the IPS logE. Use a third-party system to perform penetration testing Answer: EExplanation:Only penetration testing can confirm this. All the other options lead to inconclusive results and may still result in false negatives. QUESTION 145Which two statement about stateless firewalls is true? (Choose two) A. the Cisco ASA is implicitly stateless because it blocks all traffic by default.B. They compare the 5-tuple of each incoming packets against configurable rules.C. They cannot track connections..D. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS..E. Cisco IOS cannot implement them because the platform is Stateful by nature Answer: BCExplanation:5-tuple is: source/destination IP, ports, and protocols. Stateless firewalls cannot track connections. QUESTION 146Which three ESP fields can be encrypted during transmission? (Choose three) A. Next HeaderB. MAC Address C. PaddingD. Pad LengthE. Sequence NumberF. Security Parameter Index Answer: ACDExplanation:The last encrypted part is the Payload Data. The unencrypted parts are the Security Parameter Index and the Sequence Number. QUESTION 147Which type of PVLAN port allows host in the same VLAN to communicate directly with the other? A. promiscuous for hosts in the PVLANB. span for hosts in the PVLANC. Community for hosts in the PVLAND. isolated for hosts in the PVLAN Answer: C Explanation:Hosts in the same PVLAN Community can communicate with one another. QUESTION 148Refer to the exhibit while troubleshooting site-to-site VPN, you issued the show crypto isakamp sa command. What does the given output shows?

A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2B. IKE Phase 1 main mode has

successfully negotiate between 10.1.1.5 and10.10.10.2C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2D. IKE Phase 1 aggressive mode was create on 10.1.1.5, but it failed to negotiate with 10.10.10.2 Answer: AExplanation:The MM_NO_STATE state indicates that the phase 1 policy does not match on both sides, therefore main mode failed to negotiate. Aggressive mode is indicated by AG instead of MM. QUESTION 149Refer to the exhibit while troubleshooting site-to-site VPN, you issued the show crypto isakamp sa command. What does the given output shows?

A. IPSec Phase 2 established between 10.10.10.2 and 10.1.1.5B. IPSec Phase 1 established between 10.10.10.2 and 10.1.1.5C. IPSec Phase 2 is down due to a QM_IDLE state.D. IPSec Phase 1 is down due to a QM_IDLE state. Answer: BExplanation:An IDLE state is good and means that the connection and key exchange have taken place successfully. QM indicates that the device is ready for phase 2 (quick mode) and subsequent data transfer. QUESTION 150Refer to the exhibit. You have configured R1 and R2 as shown, but the routers are unable to establish a site-to-site VPN tunnel. What action can you take to correct the problem?



A. Edit the crypto keys on R1 and R2 to match.B. Edit the crypto isakmp key command on each router with the address value of its own interfaceC. Edit the ISAKMP policy sequence numbers on R1 and R2 to match.D. set a valid value for the crypto key lifetime on each router. Answer: AExplanation:The crypto keys don't match here. I've inferred and assumed that the destination address at the end of the "Crypto isakmp key test12345 address 10.30.30.5" line is the IP address of R1. By extension, this would produce an MM_NO_STATE state if you ran the "show crypto isakmp sa" command, as it would never connect to begin phase 1. !!!RECOMMEND!!! 1.|2017 New 210-260 Exam Dumps (PDF & VCE) 362Q&As Download: https://www.braindump2go.com/210-260.html 2.|2017 New 210-260 Study Guide Video: YouTube Video: YouTube.com/watch?v=9yy5IlptXYw