[2019-April-New100% Real Exam Questions-Braindump2go 300-208 PDF Dumps 451Q Download

2019/April Braindump2go 300-209 Exam Dumps with PDF and VCE New Updated Today! Following are some new 300-209 Exam Questions:1.|2019 Latest 300-209 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/300-209.html 2.|2019 Latest 300-209 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNRkY3M21SbTdTNDg?usp=sharing NEW QUESTIONYou are troubleshooting a site-to-site VPN issue where the tunnel is not establishing. After issuing the debug crypto ipsec command on the headend router, you see the following output. What does this output suggest?1d00h: IPSec (validate_proposal): transform proposal (port 3, trans 2, hmac_alg 2) not supported1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 01d00h: ISAKMP (0:2) SA not acceptableA. Phase 1 policy does not match on both sides.B. The Phase 2 transform set does not match on both sides.C. ISAKMP is not enabled on the remote peer.D. The crypto map is not applied on the remote peer.E. The Phase 1 transform set does not match on both sides.**Answer: B**NEW QUESTIONWhich adaptive security appliance command can be used to see a generic framework of therequirements for configuring a VPN tunnel between an adaptive security appliance and a Cisco IOS router at a remote office?A. vpnsetup site-to-site stepsB. show running-config cryptoC. show vpn-sessiondb l2lD. vpnsetup ssl-remote-access steps**Answer: A**NEW QUESTIONAfter completing a site-to-site VPN setup between two routers, application performance over the tunnel is slow. You issue the show crypto ipsec sa command and see the following output. What does this output suggest?interfacE. Tunnel100Crypto map tag: Tunnel100-head-0, local addr 10.10.10.10protected vrF. (none)local ident (addr/mask/prot/port): (10.10.10.10/255.255.255.255/47/0)remote ident (addr/mask/prot/port): (10.20.20.20/255.255.255.255/47/0) current_peer 209.165.200.230 port 500PERMIT, flags={origin_is_acl,}#pkts encaps: 34836, #pkts encrypt: 34836, #pkts digest: 34836#pkts decaps: 26922, #pkts decrypt: 19211, #pkts verify: 19211#pkts compresseD. 0, #pkts decompresseD. 0#pkts not compresseD. 0, #pkts compr. faileD. 0#pkts not decompresseD. 0, #pkts decompress faileD. 0#send errors 0, #recv errors 0A. The VPN has established and is functioning normally.B. There is an asymmetric routing issue.C. The remote peer is not receiving encrypted traffic.D. The remote peer is not able to decrypt traffic.E. Packet corruption is occurring on the path between the two peers.**Answer: E**NEW QUESTIONRefer to the exhibit. An administrator had the above configuration working with SSL protocol, but as soon as the administrator specified IPsec as the primary protocol, the Cisco AnyConnect client was not able to connect. What is the problem? A. IPsec will not work in conjunction with a group URL.B. The Cisco AnyConnect implementation does not allow the two group URLs to be the same.SSL does allow this.C. If you specify the primary protocol as IPsec, the User Group must be the exact name of the connection profile (tunnel group).D. A new XML profile should be created instead of modifying the existing profile, so that the clients force the update.**Answer: CNEW QUESTION**The Cisco AnyConnect client fails to connect via IKEv2 but works with SSL. The following error message is displayed:"Login Denied, unauthorized connection mechanism, contact your administrator"What is the most possible cause of this problem?A. DAP is terminating the connection because IKEv2 is the protocol that is being used.B. The client endpoint does not have the correct user profile to initiate an IKEv2 connection.C. The AAA server that is being used does not authorize IKEv2 as the connection mechanism.D. The administrator is restricting access to this specific user.E. The IKEv2 protocol is not enabled in the group policy of the VPN headend.**Answer: E**NEW QUESTIONThe Cisco AnyConnect client is unable to download an updated user profile from the ASA headend using IKEv2. What is the most likely cause of this problem?A. User profile updates are not allowed with IKEv2.B. IKEv2 is not enabled on the group policy.C. A new profile must be created so that the adaptive security appliance can push it to the client on the next connection attempt.D. Client Services is not enabled on the adaptive security appliance.**Answer: D**NEW QUESTIONRefer to the exhibit. The network administrator is adding a new spoke, but the tunnel is not passing traffic. What could cause this issue? A. DMVPN is a point-to-point tunnel, so there can be only one spoke.B. There is no EIGRP configuration, and therefore the second tunnel is not working.C. The NHRP authentication is failing.D. The transform set must be in transport mode, which is a requirement for DMVPN.E. The NHRP network ID is incorrect.Answer: CExplanation:
http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html#wp1055049NEW QUESTION Which two troubleshooting steps should be taken when Cisco AnyConnect cannot establish an IKEv2 connection, while SSL works fine? (Choose two.)A. Verify that the primary protocol on the client machine is set to IPsec.B. Verify that AnyConnect is enabled on the correct interface.C. Verify that the IKEv2 protocol is enabled on the group policy.D. Verify that ASDM and AnyConnect are not using the same port.E. Verify that SSL and IKEv2 certificates are not referencing the same trustpoint. **Answer: AC**NEW QUESTIONRegarding licensing, which option will allow IKEv2 connections on the adaptive security appliance?A. AnyConnect Essentials can be used for Cisco AnyConnect IKEv2 connections.B. IKEv2 sessions are not licensed.

C. The Advanced Endpoint Assessment license must be installed to allow Cisco AnyConnect IKEv2 sessions.D. Cisco AnyConnect Mobile must be installed to allow AnyConnect IKEv2 sessions.**Answer: A**NEW QUESTIONWhat action does the hub take when it receives a NHRP resolution request from a spoke for a network that exists behind another spoke?A. The hub sends back a resolution reply to the requesting spoke.B. The hub updates its own NHRP mapping.C. The hub forwards the request to the destination spoke.D. The hub waits for the second spoke to send a request so that it can respond to both spokes.**Answer: C** NEW QUESTIONA spoke has two Internet connections for failover. How can you achieve optimum failover without affecting any other router in the DMVPN cloud?A. Create another DMVPN cloud by configuring another tunnel interface that is sourced from the second ISP link.B. Use another router at the spoke site, because two ISP connections on the same router for the same hub is not allowed.C. Configure SLA tracking, and when the primary interface goes down, manually change the tunnel source of the tunnel interface.D. Create another tunnel interface with same configuration except the tunnel source, and configure the if-state nhrp and backup interface commands on the primary tunnel interface.Answer: DExplanation: **http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/xe-3s/sec-conn-dmvpn-xe-3s-book/sec-conn-dmvpn-tun-mon.pdf**!!!RECOMMEND!!!1.|2019 Latest 300-209 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/300-209.html 2.|2019 Latest 300-209 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=6IIkz7Mm6FM