[2017 New 2017 New 210-260 Exam PDF Ensure 210-260 Certification Exam Pass Successfully (21-40)

2017 July Cisco Official New Released **210-260** Dumps in Lead2pass.com!] 100% Free Download! 100% Pass Guaranteed! Lead2pass provides 100% pass 210-260 exam questions and answers for your Cisco 210-260 exam. We provide Cisco 210-260 exam questions from Lead2pass dumps and answers for the training of 210-260 practice test. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/210-260.html QUESTION 21Which command is needed to enable SSH support on a Cisco Router? A.   crypto key lock rsaB.   crypto key generate rsaC.   crypto key zeroize rsaD. crypto key unlock rsaAnswer: B QUESTION 22In which three ways does the TACACS protocol differ from RADIUS? (Choose three) A.   TACACS uses TCP to communicate with the NASB.   TACACS can encrypt the entire packet that is sent to the NASC. TACACS authenticates and authorizes simultaneously, causing fewer packets to be transmittedD.   TACACS uses UDP to communicate with the NASE.   TACACS encrypts only the password field in an authentication packetF.   TACACS support per-command authorization Answer: ABF QUESTION 23ScenarioIn this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.To access ASDM, click the ASA icon in the topology diagram.Note: Not all ASDM functionalities are enabled in this simulation.To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.   Which user authentication method is used when users login to the Clientless SSL VPN portal using https://209165.201.2/test? A.   Both Certificate and AAA with LOCAL databaseB.   AAA with RADIUS serverC.   Both Certificate and AAA with RADIUS serverD.   AAA with LOCAL databaseE.   Certificate Answer: DExplanation:This can be seen from the Connection Profiles Tab of the Remote Access VPN configuration,where the alias of test is being used.   QUESTION 24ScenarioIn this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.To access ASDM, click the ASA icon in the topology diagram.Note: Not all ASDM functionalities are enabled in this simulation.To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.   When users login to the Clientless SSL VPN using https://209.165.201.2/test, which group policy will be applied? A.   testB.   SalesC.   DefaultRAGroupD.   DefaultWEBVPNGroupE.   clientlessF.   DFTGrpPolicy Answer: B Explanation:First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias: Then hit the ?edit? button and you can clearly see the Sales Group Policy being applied.   QUESTION 25ScenarioIn this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.To access ASDM, click the ASA icon in the topology diagram.Note: Not all ASDM functionalities are enabled in this simulation.To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.   Which two statements regarding the ASA VPN configurations are correct? (Choose two) A.   The Inside-SRV bookmark has not been applied to the Sales group policyB.   The ASA has a certificate issued by an external Certificate Authority associated to the ASDM_Trustpoint1C.   The Inside-SRV bookmark references the https://10.x.x.x URLD.   Any Connect, IPSec IKEv1 and IPSec IKEv2 VPN access is enabled on the outside interfaceE.   Only Clientless SSL VPN VPN access is allowed with the Sales group PolicyF.   The DefaultWEBVPNGroup Connection Profile is using the AAA with Radius server method Answer: EFExplanation:In the real If appear in the option answers an ip like https://10... URL and not https://192.168.1.2 URL then the answers will be EF. QUESTION 26ScenarioIn this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.To access ASDM, click the ASA icon in the topology diagram.Note: Not all ASDM functionalities are enabled in this simulation.To see all the menu options available on the left navigation pane, you may also need to un-expand the expanded menu first.   Which four tunneling protocols are enabled in the DfltGrpPolicy group policy? (choose four) A.   IPsec IKEv1B.   IPsec IKEv2C.   L2TP/IPsecD. Clientless SSL VPNE.   SSL VPN ClientF.   PPTP Answer: ABCDExplanation:By clicking one the Configuration-> Remote Access -> Clientless CCL VPN Access-> Group Policies tab you can view the DfltGrpPolicy protocols as shown below: QUESTION 27ScenarioGiven the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.New additional connectivity requirements: - Currently, the ASA configurations only allow on the Inside and DMZ networks to access any hosts on the Outside. Your task is to use ASDM to configure the ASA to also allow any host only on the Outside to HTTP to the DMZ server. The hosts on the Outside will need to use the 209.165.201.30 public IP address when HTTPing to the DMZ server.- Currently, hosts on the ASA higher security level interfaces are not able to ping any hosts on the lower security level interfaces. Your task in this simulation is to use ASDM to enable the ASA to dynamically allow the echo-reply responses back through the ASA. Once the correct ASA configurations have been

configured: - You can test the connectivity tohttp://209.165.201,30from the Outside PC browser.- You can test the pings to the Outside (www.cisco.com) by opening the inside PC command prompt window.   In this simulation, only testing pings to www.cisco.com will work. To access ASDM, click the ASA icon in the topology diagram.To access the Firefox Browser on the Outside PC, click the Outside PC icon in the topology diagram.To access the Command prompt on the Inside PC, click the Inside PC icon in the topology diagram. Note:After you make the configuration changes in ASDM, remember to click Apply to apply the configuration changes.Not all ASDM screens are enabled in this simulation, if some screen is not enabled, try to use different methods to configure the ASA to meet the requirements.In this simulation, some of the ASDM screens may not look and function exactly like the real ASDM. Answer: Step 1: Firewall, Configuration, NAT Rules, Name=WebSvr, IP version IPv4, IP address=172.16.1.2 Static NAT=209.165.201.30Step 2: Firewall, Config, Access Rules, Interface=Outside, Action=Permit, Source=any, Destination=209.165.201.30, Service=tcp/httpStep 3: Firewall, Config, Service policy Rules, Click Global Policy and edit, Rule Action tab, Click ICMP and applyStep 4: Ping www.cisco.com from Inside PCStep 5: Type http://209.165.201.30 in web browser in the Outside PC Explanation:First, for the HTTP access we need to creat a NAT object. Here I called it HTTP but it can be given any name.   Then, create the firewall rules to allow the HTTP access: You can verify using the outside PC to HTTP into 209.165.201.30.For step two, to be able to ping hosts on the outside, we edit the last service policy shown below: And then check the ICMP box only as shown below, then hit Apply.   After that is done, we can ping www.cisco.com again to verify: QUESTION 28What is the purpose of the Integrity component of the CIA triad? A.   to ensure that only authorized parties can modify dataB.   to determine whether data is relevantC.   to create a process for accessing dataD.   to ensure that only authorized parties can view data Answer: A QUESTION 29Which two statements about Telnet access to the ASA are true? (Choose two). A.   You may VPN to the lowest security interface to telnet to an inside interface.B.   You must configure an AAA server to enable Telnet.C.   You can access all interfaces on an ASA using Telnet.D.   You must use the command virtual telnet to enable Telnet.E.   Best practice is to disable Telnet and use SSH. Answer: AE QUESTION 30Which protocol provides security to Secure Copy? A.   IPsecB.   SSHC.   HTTPSD.   ESP Answer: B QUESTION 31A clientless SSL VPN user who is connecting on a Windows Vista computer is missing the menu option for Remote Desktop Protocol on the portal web page. Which action should you take to begin troubleshooting? A.   Ensure that the RDP2 plug-in is installed on the VPN gatewayB.   Reboot the VPN gatewayC.   Instruct the user to reconnect to the VPN gatewayD.   Ensure that the RDP plug-in is installed on the VPN gateway Answer: D QUESTION 32Which security zone is automatically defined by the system? A.   The source zoneB.   The self zoneC.   The destination zoneD.   The inside zone Answer: B QUESTION 33What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.) A.   The Internet Key Exchange protocol establishes security associationsB.   The Internet Key Exchange protocol provides data confidentialityC.   The Internet Key Exchange protocol provides replay detectionD.   The Internet Key Exchange protocol is responsible for mutual authentication Answer: Answer: AD QUESTION 34Which address block is reserved for locally assigned unique local addresses? A.   2002::/16B.   FD00::/8C.   2001::/32D.   FB00::/8 Answer: B QUESTION 35What is a possible reason for the error message? Router(config)#aaa server?% Unrecognized command A.   The command syntax requires a space after the word "server"B.   The command is invalid on the target deviceC.   The router is already running the latest operating systemD.   The router is a new device on which the aaa new-model command must be applied before continuing Answer: D QUESTION 36Which statements about smart tunnels on a Cisco firewall are true? (Choose two.) A.   Smart tunnels can be used by clients that do not have administrator privilegesB.   Smart tunnels support all operating systemsC.   Smart tunnels offer better performance than port forwardingD.   Smart tunnels require the client to have the application installed locally Answer: ADExplanation:Smart Tunnel is also used to provide remote access to web applications that are difficult to rewrite, such as proprietary, non-standards-based Java, Java Script, or Flash animations. Smart Tunnel also supports Single Sign-On to web applications that require either form-based POST parameters, http basic, FTP, or NTLM authenticationSmart Tunnel can also co-exist with a Full-Tunnel VPN Client. For example, an employee can connect to the company network by using Full-Tunnel VPN Client, while simultaneously connecting to a vendor network by using Smart Tunnel.Smart Tunnel Advantages over Port-Forwarding, Plug-insSmart Tunnel offers better performance than browser plug-ins.Port forwarding is the legacy technology for supporting TCP-based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.Smart Tunnel does not require users to have administrator privileges.Smart Tunnel does not require the administrator to know application port numbers in advance. QUESTION 37Which option describes information that must be considered when you apply an access list to a physical interface? A.   Protocol used for filteringB.   Direction of the access classC.   Direction of the access groupD.   Direction of the access list Answer: C QUESTION 38Which source port does IKE use when NAT has been detected between two VPN gateways? A.   TCP 4500B.   TCP 500C.   UDP 4500D.   UDP 500 Answer: C QUESTION 39Which of the following are features of IPsec transport mode? (Choose three.) A.   IPsec transport mode is used between end stationsB.

IPsec transport mode is used between gatewaysC.   IPsec transport mode supports multicastD.   IPsec transport mode supports unicastE.   IPsec transport mode encrypts only the payloadF.   IPsec transport mode encrypts the entire packet Answer: ADE Explanation:IPSec Transport ModeIPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.Transport mode provides the protection of our data, also known as IP Payload, and consists of TCP/UDP header + Data, through an AH or ESP header. The payload is encapsulated by the IPSec headers and trailers. The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPsec trailer to be restored when the packet is decrypted.IPSec transport mode is usually used when another tunneling protocol (like GRE) is used to first encapsulate the IP data packet, then IPSec is used to protect the GRE tunnel packets. IPSec protects the GRE tunnel traffic in transport mode. QUESTION 40Which command causes a Layer 2 switch interface to operate as a Layer 3 interface? A.   no switchport nonnegotiateB.   switchportC.   no switchport mode dynamic autoD.   no switchport Answer: D Lead2pass is the leader in 210-260 certification test questions with training materials for Cisco 210-260 exam dumps. Lead2pass Cisco training tools are constantly being revised and updated. We 100% guarantee Cisco 210-260 exam questions with quality and reliability which will help you pass Cisco 210-260 exam. **210-260** new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDRVJLdVdkMjFoQVk 2017 Cisco **210-260** exam dumps (All 265 Q&As) from Lead2pass: http://www.lead2pass.com/210-260.html [100% Exam Pass Guaranteed]