[Lead2pass New Lead2pass Latest Cisco 300-209 Exam Questions Free Downloading (261-280)

2017 November Cisco Official New Released 300-209 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
You can prepare for Cisco 300-209 exam with little effort because Lead2pass is now at your service to act as a guide to pass Cisco 300-209 exam. Our Cisco 300-209 braindumps are rich in variety. We offer Cisco 300-209 PDF dumps and Cisco 300-209 VCE. Both are the newest version. Following questions and answers are all new published by Cisco Official Exam Center: https://www.lead2pass.com/300-209.html QUESTION 261Refer to the exhibit. An engineer encounters a debug message. Which action can the engineer take to eliminate this error message? A. Use stronger encryption suite.B. Correct the VPN peer address. C. Make adjustment to IPSec replay window.D. Change the preshared key to match.Answer: C QUESTION 262Which two changes must be made to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two) A. Disable EIGRP next-hop-self on the hub.B. Enable EIGRP next-hop-self on the hub.C. Add NHRP shortcuts on the hub.D. Add NHRP redirects on the hub.E. Add NHRP redirects on the spoke. Answer: AD QUESTION 263Refer to the exhibit. VPN load balancing provides a way to distribute remote access, IPsec, and SSL VPN connections across multiple security appliances. Which remote access client types does the load balancing feature support? A. IPsec site-to-site tunnelsB. L2TP over IPsecC. OpenVPND. Cisco AnyConnect Secure Mobility Client Answer: D QUESTION 264Which two are features of GETVPN but not DMVPN and FlexVPN? (Choose two.) A. sequence numbers that enable scalable replay checking CD protocolB. no requirement for an overlay routing protocol.C. design for use over public or private.D. WAN enabled use of ESP or AH.E. one IPsec SA for all encrypted traffic. Answer: BE QUESTION 265Refer to the exhibit. A new NOC engineer, while viewing a real-time log from an SSL VPN tunnel, has a question about a line in the log. The IP address 172.26.26.30 is attached to which interface in the network? A. the Cisco ASA physical interfaceB. the physical interface of the end userC. the Cisco ASA SSL VPN tunnel interfaceD. the SSL VPN tunnel interface of the end user Answer: B QUESTION 266You have been using pre-shared keys for IKE authentication on your VPN. Your network has grown rapidly, and now you need to create VPNs with numerous IPsec peers. How can you enable scaling to numerous IPsec peers? A. Migrate to external CA-based digital certificate authentication.B. Migrate to a load-balancing server.C. Migrate to a shared license server.D. Migrate from IPsec to SSL VPN client extended authentication. Answer: A QUESTION 267Which statement is correct concerning the trusted network detection (TND) feature? A. The Cisco AnyConnect 3.0 Client supports TND on Windows, Mac, and Linux platforms.B. With TND, one result of a Cisco Secure Desktop basic scan on an endpoint is to determine whether a device is a member of a trusted or an untrusted network.C. If enabled, and a CSD scan determines that a host is a member of an untrusted network, an administrator can configure the TND feature to prohibit an end user from launching the Cisco AnyConnect VPN Client.D. When the user is inside the corporate network, TND can be configured to automatically disconnect a Cisco AnyConnect session. Answer: DExplanation: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administrat ion/guide/ac03features.htmlTrusted Network DetectionTrusted Network Detection (TND) gives you the ability to have AnyConnect automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network) and start the VPN connection when the user is outside the corporate network (the untrusted network). This feature encourages greater security awareness by initiating a VPN connection when the user is outside the trusted network.If AnyConnect is also running Start Before Logon (SBL), and the user moves into the trusted network, the SBL window displayed on the computer automatically closes. TND does not interfere with the ability of the user to manually establish a VPN connection. It does not disconnect a VPN connection that the user starts manually in the trusted network. TND only disconnects the VPN session if the user first connects in an untrusted network and moves into a trusted network. For example, TND disconnects the VPN session if the user makes a VPN connection at home and then moves into the corporate office.Because the TND feature controls the AnyConnect GUI and automatically initiates connections, the GUI should run at all times. If the user exits the GUI, TND does not automatically start the VPN connection.You configure TND in the AnyConnect profile. No changes are required to the ASA configuration. QUESTION 268Refer to the exhibit. A NOC engineer needs to tune some postlogin parameters on an SSL VPN tunnel. From the information shown, where should the engineer navigate to, in order to find all the postlogin session parameters? A. "engineering" Group PolicyB. "contractor" Connection ProfileC. DefaultWEBVPNGroup Group PolicyD. DefaultRAGroup Group PolicyE. "engineer1" AAA/Local Users Answer: A Explanation:http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1054618The policy group is a container that defines the presentation of the portal and the permissions for resources that are configured for a group of remote users. Entering the policy group command places the router in webvpn group policy configuration mode. After it is configured, the group policy is attached to the SSL VPN context configuration by configuring the default-group-policy command.The following tasks are

accomplished in this configuration:The presentation of the SSL VPN portal page is configured.A NetBIOS server list is referenced. A port-forwarding list is referenced.The idle and session timers are configured.A URL list is referenced. QUESTION 269Which statement about plug-ins is false? A. Plug-ins do not require any installation on the remote system.B. Plug-ins require administrator privileges on the remote system.C. Plug-ins support interactive terminal access.D. Plug-ins are not supported on the Windows Mobile platform. Answer: BExplanation: http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/ deployhtml#wp1162435Plug-insThe security appliance supports Java plug-ins for clientless SSL VPN connections. Plug-ins are Java programs that operate in a browser. These plug-ins include SSH/Telnet, RDP, VNC, and Citrix.Per the GNU General Public License (GPL), Cisco redistributes plug-ins without making any changes to them.Per the GPL, Cisco cannot directly enhance these plug-ins. To use plug-ins you must install Java Runtime Environment (JRE) 1.4.2.x or greater. You must also use a compatible browser specified here: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpncompatibility.html QUESTION 270When attempting to tunnel FTP traffic through a stateful firewall that might be performing NAT or PAT, which type of VPN tunneling should you use to allow the VPN traffic through the stateful firewall? A. clientless SSL VPNB. IPsec over TCPC. smart tunnelD. SSL VPN plug-ins Answer: BExplanation:IP Security (IPSec) over Transmission Control Protocol (TCP) enables a VPN Client to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, User Datagram Protocol (UDP) 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and it enables secure tunneling through both Network Address Translation (NAT) and Port Address Translation (PAT) devices and firewalls QUESTION 271Refer to the exhibit. The ABC Corporation is changing remote-user authentication from pre-shared keys to certificate-based authentication. For most employee authentication, its group membership (the employees) governs corporate access. Certain management personnel need access to more confidential servers. Access is based on the group and name, such as finance and level_2. When it is time to pilot the new authentication policy, a finance manager is able to access the department-assigned servers but cannot access the restricted servers. As the network engineer, where would you look for the problem? A. Check the validity of the identity and root certificate on the PC of the finance manager. B. Change the Management Certificate to Connection Profile Maps > Rule Priority to a number that is greater than 10.C. Check if the Management Certificate to Connection Profile Maps > Rules is configured correctly.D. Check if the Certificate to Connection Profile Maps > Policy is set correctly. Answer: D QUESTION 272Refer to the exhibit. While configuring a site-to-site VPN tunnel, a new NOC engineer encounters the Reverse Route Injection parameter. Assuming that static routes are redistributed by the Cisco ASA to the IGP, what effect does enabling Reverse Route Injection on the local Cisco ASA have on a configuration? A. The local Cisco ASA advertises its default routes to the distant end of the site-to-site VPN tunnel.B. The local Cisco ASA advertises routes from the dynamic routing protocol that is running on the local Cisco ASA to the distant end of the site-to-site VPN tunnel.C. The local Cisco ASA advertises routes that are at the distant end of the site-to-site VPN tunnel.D. The local Cisco ASA advertises routes that are on its side of the site-to-site VPN tunnel to the distant end of the site-to-site VPN tunnel. Answer: C Explanation:http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080 9d07de.shtml QUESTION 273Refer to the exhibit. The "level_2" digital certificate was installed on a laptop. What can cause an "invalid not active" status message? A. On first use, a CA server-supplied passphrase is entered to validate the certificate.B. A "newly installed" digital certificate does not become active until it is validated by the peer device upon its first usage.C. The user has not clicked the Verify button within the Cisco VPN Client.D. The CA server and laptop PC clocks are out of sync. Answer: DExplanation: http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.htmlCertificates have a date and time that they become valid and that they expire. When the security appliance enrolls with a CA and gets a certificate, the security appliance checks that the current time is within the valid range for the certificate. If it is outside that range, enrollment fails.Same would apply to communication between ASA and PC QUESTION 274Refer to the exhibit. In the CLI snippet that is shown, what is the function of the deny option in the access list? A. When set in conjunction with outbound connection-type bidirectional, its function is to prevent the specified traffic from being protected by the crypto map entry.B. When set in conjunction with connection-type originate-only, its function is to instruct the Cisco ASA to deny specific inbound traffic if it is not encrypted.C. When set in conjunction with outbound connection-type answer-only, its function is to instruct the Cisco ASA to deny specific outbound traffic if it is not encrypted.D. When set in conjunction with connection-type originate-only, its function is to cause all IP traffic that matches the specified conditions to be protected by the crypto map. Answer: A QUESTION 275After adding a remote-access IPsec tunnel via the VPN wizard, an administrator needs to tune the IPsec policy parameters. Where is the correct place to tune the IPsec policy parameters in Cisco ASDM? A. IPsec user profileB. Crypto MapC. Group PolicyD. IPsec PolicyE. IKE Policy Answer: B QUESTION 276Refer to the exhibit. A new NOC engineer is troubleshooting a VPN connection.Which statement about

the fields within the Cisco VPN Client Statistics screen is correct? A. The ISP-assigned IP address of 10.0.21.1 is assigned to the VPN adapter of the PC.B. The IP address of the security appliance to which the Cisco VPN Client is connected is 192.168.1.2.C. CorpNet is the name of the Cisco ASA group policy whose tunnel parameters the connection is using.D. The ability of the client to send packets transparently and unencrypted through the tunnel for test purposes is turned off.E. With split tunneling enabled, the Cisco VPN Client registers no decrypted packets. Answer: B QUESTION 277What is a valid reason for configuring a list of backup servers on the Cisco AnyConnect VPN Client profile? A. to access a backup authentication serverB. to access a backup DHCP serverC. to access a backup VPN serverD. to access a backup CA server Answer: C QUESTION 278Your corporate finance department purchased a new non-web-based TCP application tool to run on one of its servers. Certain finance employees need remote access to the software during nonbusiness hours. These employees do not have "admin" privileges to their PCs.What is the correct way to configure the SSL VPN tunnel to allow this application to run? A. Configure a smart tunnel for the application.B. Configure a "finance tool" VNC bookmark on the employee clientless SSL VPN portal.C. Configure the plug-in that best fits the application.D. Configure the Cisco ASA appliance to download the Cisco AnyConnect SSL VPN Client to the finance employee each time an SSL VPN tunnel is established. Answer: A QUESTION 279A temporary worker must use clientless SSL VPN with an SSH plug-in, in order to access the console of an internal corporate server, the projects.xyz.com server. For security reasons, the network security auditor insists that the temporary user is restricted to the one internal corporate server, 10.0.4.18. You are the network engineer who is responsible for the network access of the temporary user.What should you do to restrict SSH access to the one projects.xyz.com server? A. Configure access-list temp_user_acl extended permit TCP any host 10.0.4.18 eq 22.B. Configure access-list temp_user_acl standard permit host 10.0.4.18 eq 22.C. Configure access-list temp_acl webtype permit url ssh://10.0.4.18.D. Configure a plug-in SSH bookmark for host 10.0.4.18, and disable network browsing on the clientless SSL VPN portal of the temporary worker. Answer: C QUESTION 280Refer to the exhibit. A junior network engineer configured the corporate Cisco ASA appliance to accommodate a new temporary worker. For security reasons, the IT department wants to restrict the internal network access of the new temporary worker to the corporate server, with an IP address of 10.0.4.10. After the junior network engineer finished the configuration, an IT security specialist tested the account of the temporary worker. The tester was able to access the URLs of additional secure servers from the WebVPN user account of the temporary worker.What did the junior network engineer configure incorrectly? A. The ACL was configured incorrectly.B. The ACL was applied incorrectly or was not applied.C. Network browsing was not restricted on the temporary worker group policy.D. Network browsing was not restricted on the temporary worker user policy. Answer: B Cisco Certification 300-209 certificate are those engaged in IT industry's dream. You need to choose the professional training by Lead2pass Cisco 300-209 dumps. Lead2pass will be with you, and to ensure the success wherever you may increase pursuit your career. Let Lead2pass take all your heart, let the dream to reality! More 300-209 new questions (with images) on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDYnF5Vk16OS1tc1E 2017 Cisco 300-209 exam dumps (All 319 Q&As) from Lead2pass: https://www.lead2pass.com/300-209.html [100% Exam Pass Guaranteed]