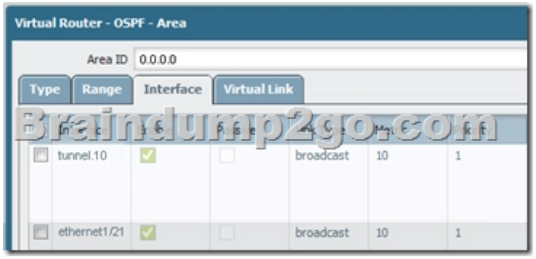
[NEW PCNSE7 PDFPalo Alto Networks 131q PCNSE7 Dumps Free Download in Braindump2go[51-60

2017 June New Updated PCNSE7 Exam Dumps with PDF and VCE Free Shared in www.Braindump2go.com Today!100% Real Exam Questions! 100% Exam Pass Guaranteed!1.|2017 New PCNSE7 PDF and PCNSE7 VCE 131Q&As Download: http://www.braindump2go.com/pcnse7.html 2.|2017 New PCNSE7 Questions and Answers PDF Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNZUpkbFJ5WVdSaVk?usp=sharing QUESTION 51Which Public Key infrastructure component is used to authenticate users for GlobalProtect when the Connect Method is set to pre-logon? A. Certificate revocation listB. Trusted root certificateC. Machine certificateD. Online Certificate Status Protocol Answer: C Explanation:The GlobalProtect pre-logon connect method is a feature that enables GlobalProtect to authenticate the agent and establish the VPN tunnel to the GlobalProtect gateway using a pre-installed machine certificate before the user has logged in. https://www.paloaltonetworks.com/documentation/60/globalprotect/global_protect_6-0/globalprotect-quick-configs/remote-access-vpn-with-pre-logon QUESTION 52The company's Panorama server (IP 10.10.10.5) is not able to manage a firewall that was recently deployed. The firewall's dedicated management port is being used to connect to the management network.Which two commands may be used to troubleshoot this issue from the CLI of the new firewall? (Choose two) A. test panoramas-connect 10.10.10.5B. show panoramas-statusC. show arp all I match 10.10.10.5D. topdump filter "host 10.10.10.5E. debug dataplane packet-diag set capture on Answer: BDExplanation:B: The show panorama-status command shows the Panorama connection status.Sample Output The following command shows information about the Panorama connection.username@hostname> show panorama-statusPanorama Server 1 : 10.1.7.90State : Unknownusername@hostname>D: IssueThe Managed Devices show not connected to Panorama and are not able to establish a new connection to Panorama.The Packet Capture on Panorama Management Interface shows SYN packets received from devices on port 3978, but no SYN ACK is sent from Panorama.> tcpdump filter "port 3978"> view-pcap mgmt-pcap mgmt.pcap
https://live.paloaltonetworks.com/t5/Management-Articles/Managed-Devices-Unable-to-Establish-Connections-to-Panorama/ta-p/53248
https://www.paloaltonetworks.jp/content/dam/paloaltonetworks-com/en_US/assets/pdf/technical-documentation/pan-os-5x/CLI_Reference_Guide-Panorama-5.1_PAN-OS-5.0.pdf QUESTION 53Which three log-forwarding destinations require a server profile to be configured? (Choose three) A. SNMP TrapB. EmailC. RADIUSD. KerberosE. PanoramaF. Syslog Answer: ABF Explanation:Enable a Log Forwarding Profile (see step 4 below).1. Select Objects > Log Forwarding Profile and Add a new security profile group.2. Give the profile group a descriptive Name to help identify it when adding the profile to security policies or security zones.3. If the firewall is in Multiple Virtual System Mode, enable the profile to be Shared by all virtual systems.4. Add settings for the Traffic logs, Threat logs, and WildFire logs:Select the Panorama check box for the severity of the Traffic, Threat, or WildFire logs that you want to be forwarded to Panorama.Specify logs that you want to forward to additional destinations: SNMP Trap destinations, Email servers, or Syslog servers.5. Click OK to save the log forwarding profile.
https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/reports-and-logging/log-forwarding-profiles.html QUESTION 54Which setting allow a DOS protection profile to limit the maximum concurrent sessions from a source IP address? A. Set the type to Aggregate, clear the session's box and set the Maximum concurrent Sessions to 4000.B. Set the type to Classified, clear the session's box and set the Maximum concurrent Sessions to 4000.C. Set the type Classified, check the Sessions box and set the Maximum concurrent Sessions to 4000.D. Set the type to aggregate, check the Sessions box and set the Maximum concurrent Sessions to 4000. Answer: C QUESTION 55A company has a web server behind a Palo Alto Networks next-generation firewall that it wants to make accessible to the public at 1.1.1.1. The company has decided to configure a destination NAT Policy rule.Given the following zone information:DMZ zone: DMZ-L3Public zone: Untrust-L3Guest zone: Guest-L3Web server zone: Trust-L3Public IP address (Untrust-L3): 1.1.1.1Private IP address (Trust-L3): 192.168.1.50What should be configured as the destination zone on the Original Packet tab of NAT Policy rule? A. Untrust-L3B. DMZ-L3C. Guest-L3D. Trust-L3 Answer: AExplanation:Create the NAT policy.1. Select Policies > NAT and click Add.2. Enter a descriptive Name for the policy.3. On the Original Packet tab, select the zone you created for your internal network in the Source Zone section (click Add and then select the zone) and the zone you created for the external network from the Destination Zone drop down.4. On the Translated Packet tab, select Dynamic IP And Port from the Translation Type drop-down in the Source Address Translation section of the screen and then click Add. Select the address object you just created.5. Click OK to save the NAT policy.
https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/getting-started/configure-nat-policies QUESTION 56Which two options are required on an M-100 appliance to configure it as a Log Collector? (Choose two) A. From the Panorama tab of the

Panorama GUI select Log Collector mode and then commit changesB. Enter the command request system system-mode logger then enter Y to confirm the change to Log Collector mode.C. From the Device tab of the Panorama GUI select Log Collector mode and then commit changes.D. Enter the command logger-mode enable the enter Y to confirm the change to Log Collector mode.E. Log in the Panorama CLI of the dedicated Log Collector Answer: BEExplanation:Step 1 (E): Access the Command Line Interface (CLI) on the M-100 appliance.When prompted, log in to the appliance.Step 2 (B): Switch from Panorama Mode to Log Collector Mode.1. To switch to Log Collector mode, enter the following command:request system logger-mode logger2. Enter Yes to confirm the change to Log Collector mode. The appliance will reboot. If you see a CMS Login prompt, press Enter without typing a username or password. When the Panorama login prompt appears, enter the default admin account and the password assigned during initial configuration.
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance#91340 QUESTION 57Click the Exhibit button. An administrator has noticed a large increase in bittorrent activity. The administrator wants to determine where the traffic is going on the company.

What would be the administrator's next step? A. Right-Click on the bittorrent link and select Value from the context menuB. Create a global filter for bittorrent traffic and then view Traffic logs.C. Create local filter for bittorrent traffic and then view Traffic logs.D. Click on the bittorrent application link to view network activity Answer: DExplanation:The application filter is a dynamic item that is created by selecting filter options (Category, Subcategory, Technology) in the application browser. Any new applications coming to PAN-OS in a content update that match the same filters, the set will automatically be added to the Application Filter created. For example, when a 'peer-to-peer' is selected as a Technology Filter, that filter will automatically update if a new application gets added to that category in the latest content package.
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Block-Traffic-Based-on-Application-Filters-with-an/ta-p/59965 QUESTION 58Support for which authentication method was added in PAN-OS 7.0? A. RADIUSB. LDAPC. DiameterD. TACACS+ Answer: DExplanation:Devices now support Terminal Access Controller Access-Control System Plus (TACACS+) protocol for authenticating administrative users. TACACS+ provides greater security than RADIUS insofar as it encrypts usernames and passwords (instead of just passwords), and is also more reliable (it uses TCP instead of UDP).
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os-release-notes/pan-os-7-0-release-information/authentication-features#91847 QUESTION 59Click the Exhibit button below, A firewall has three PBF rules and a default route with a next hop of 172.20.10.1 that is configured in the default VR. A user named Will has a PC with a 192.168.10.10 IP address.He makes an HTTPS connection to 172.16.10.20.Which is the next hop IP address for the HTTPS traffic from Will's PC?

A. 172.20.30.1B. 172.20.40.1C. 172.20.20.1D. 172.20.10.1 Answer: C QUESTION 60Site-A and Site-B have a site-to-site VPN set up between them. OSPF is configured to dynamically create the routes between the sites. The OSPF configuration in Site-A is configured properly, but the route for the tunner is not being established. The Site-B interfaces in the graphic are using a broadcast Link Type. The administrator has determined that the OSPF configuration in Site-B is using the wrong Link Type for one of its interfaces.Which Link Type setting will correct the error?



A. Set tunnel. 1 to p2pB. Set tunnel. 1 to p2mpC. Set Ethernet 1/1 to p2mpD. Set Ethernet 1/1 to p2p Answer: A !!!RECOMMEND!!! 1.|2017 New PCNSE7 PDF and PCNSE7 VCE 131Q&As Download: http://www.braindump2go.com/pcnse7.html 2.|2017 New PCNSE7 Study Guide Video: YouTube Video: YouTube.com/watch?v=or7j9-27yWc