[NEW PCNSE7 PDFPCNSE7 Exam Questions and Answers New from Braindump2go[31-40

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 31A Palo Alto Networks firewall is being targeted by an NTP Amplification attack and is being flooded with tens thousands of bogus UDP connections per second to a single destination IP address and post.Which option when enabled with the correction threshold would mitigate this attack without dropping legitirnate traffic to other hosts insides the network? A. Zone Protection Policy with UDP Flood ProtectionB. QoS Policy to throttle traffic below maximum limitC. Security Policy rule to deny trafic to the IP address and port that is under attackD. Classified DoS Protection Policy using destination IP only with a Protect action Answer: DExplanation:Step 1: Configure a DoS Protection profile for flood protection.1. Select Objects > Security Profiles > DoS Protection and Add a profile Name.2. Select Classified as the Type.3. For Flood Protection, select the check boxes for all of the following types of flood protection: SYN Flood UDP Flood ICMP Flood ICMPv6 Flood Other IP FloodStep 2: Configure a DoS Protection policy rule that specifies the criteria for matching the incoming traffic.This step include: (Optional) For Destination Address, select Any or enter the IP address of the device you want to protect.
https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/policy/configure-dos-protection-against-flooding-of-new-sessions QUESTION 32Which Security Policy Rule configuration option disables antivirus and anti-spyware scanning of server-to-client flows only? A. Disable Server Response InspectionB. Apply an Application OverrideC. Disable HIP ProfileD. Add server IP Security Policy exception Answer: AExplanation:In the Other Settings section, select the option to Disable Server Response Inspection. This setting disables the antivirus and anti-spyware scanning on the server-side responses, and thus reduces the load on the firewall.https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/getting-started/set-up-basic-security-policies QUESTION 33Which three options are available when creating a security profile? (Choose three) A. Anti-MalwareB. File BlockingC. Url FilteringD. IDS/ISPE. Threat PreventionF. Antivirus Answer: BCFExplanation:Using the URL Category as match criteria allows you to customize security profiles (antivirus, anti-spyware, vulnerability, file-blocking, Data Filtering, and DoS) on a per-URL-category basis. QUESTION 34Given the following table. Which configuration change on the firewall would cause it to use 10.66.24.88 as the next hop for the 192.168.93.0/30 network? A. Configuring the administrative Distance for RIP to be lower than that of OSPF Int.B. Configuring the metric for RIP to be higher than that of OSPF Int.C. Configuring the administrative Distance for RIP to be higher than that of OSPF Ext.D. Configuring the metric for RIP to be lower than that OSPF Ext. Answer: AExplanation:The best route is then selected among them based on Administrative Distance (AD) value of routing protocols which routes came from and that route is marked with flag A, stating that it is the Active route.Administrative distance (AD) is an arbitrary numerical value assigned to dynamic routes, static routes and directly-connected routes. The value is used by vendor-specific routers to rank routes from most preferred to least preferred. When multiple paths to the same destination are available, the router uses the route with the lowest administrative distance and inserts the preferred route into its routing table.
https://live.paloaltonetworks.com/t5/Management-Articles/Routing-Table-has-Multiple-Prefixes-for-the-Same-Route/ta-p/54781 QUESTION 35A company hosts a publically accessible web server behind a Palo Alto Networks next generation firewall with the following configuration information.- Users outside the company are in the "Untrust-L3" zone- The web server physically resides in the "Trust-L3" zone.- Web server public IP address: 23.54.6.10- Web server private IP address: 192.168.1.10Which two items must be NAT policy contain to allow users in the untrust-L3 zone to access the web server? (Choose two) A. Untrust-L3 for both Source and Destination zoneB. Destination IP of 192.168.1.10C. Untrust-L3 for Source Zone and Trust-L3 for Destination ZoneD. Destination IP of 23.54.6.10 Answer: AD QUESTION 36Which two interface types can be used when configuring GlobalProtect Portal?(Choose two) A. Virtual WireB. LoopbackC. Layer 3D. Tunnel Answer: BCExplanation:GlobalProtect portal requires a Layer 3 or loopback interface for GlobalProtect clients to connect to.
https://www.paloaltonetworks.com/documentation/62/globalprotect/globalprotect-admin-guide/set-up-the-globalprotect-infrastructure/create-interfaces-and-zones-for-globalprotect QUESTION 37What can missing SSL packets when performing a packet capture on dataplane interfaces? A. The packets are hardware offloaded to the offloaded processor on the dataplaneB. The missing packets are offloaded to the management plane CPUC. The packets are not captured because they are encryptedD. There is a hardware problem with offloading FPGA on the management plane Answer: A QUESTION 38A network Administrator needs to view the default action for a specific spyware signature. The administrator follows the tabs and menus through Objects> Security Profiles>

Anti- Spyware and select default profile.What should be done next? A. Click the simple-critical rule and then click the Action drop-down list.B. Click the Exceptions tab and then click show all signatures.C. View the default actions displayed in the Action column.D. Click the Rules tab and then look for rules with "default" in the Action column. Answer: BExplanation:All Anti-spyware and Vulnerability Protection signatures have a default action defined by Palo Alto Networks. You can view the default action by navigating to Objects > Security Profiles > Anti-Spyware or Objects > Security Profiles >Vulnerability Protection and then selecting a profile. Click the Exceptions tab and then click Show all signatures and you will see a list of the signatures with the default action in the Action column. To change the default action, you must create a new profile and then create rules with a non-default action, and/or add individual signature exceptions to Exceptions in the profile.
https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/threat-prevention/set-up-antivirus-anti-spyware-and-vulnerability-protection.html QUESTION 39How does Panorama handle incoming logs when it reaches the maximum storage capacity? A. Panorama discards incoming logs when storage capacity full.B. Panorama stops accepting logs until licenses for additional storage space are appliedC. Panorama stops accepting logs until a reboot to clean storage space.D. Panorama automatically deletes older logs to create space for new ones. Answer: DExplanation:When Panorama reaches the maximum capacity, it automatically deletes older logs to create space for new ones.
https://www.paloaltonetworks.com/documentation/70/panorama/panorama_adminguide/set-up-panorama/determine-panorama-log-storage-requirements QUESTION 40Which three function are found on the dataplane of a PA-5050? (Choose three) A. Protocol DecoderB. Dynamic routingC. ManagementD. Network ProcessingE. Signature Match Answer: BDEExplanation:In these devices, dataplane zero, or dp0 for short, functions as the master dataplane and determines which dataplane will be used as the session owner that is responsible for processing and inspection. The data plane provides all data processing and security detection and enforcement, including:* (B) All networking connectivity, packet forwarding, switching, routing, and network address translation* Application identification, using the content of the applications, not just port or protocol* SSL forward proxy, including decryption and re-encryption* Policy lookups to determine what security policy to enforce and what actions to take, including scanning for threats, logging, and packet marking* Application decoding, threat scanning for all types of threats and threat prevention* Logging, with all logs sent to the control plane for processing and storageE: The following diagram depicts both the hardware and software architecture of the next-generation firewall Incorrect Answers:C: Management is done in the control plane.
https://www.niap-ccevs.org/st/st_vid10392-st.pdf !!!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