[NEW PCNSE7 PDFPCNSE7 Dump New Updated Version Free Download - Braindump2go[21-30

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 21Which two methods can be used to mitigate resource exhaustion of an application server? (Choose two) A. Vulnerability ObjectB. DoS Protection Profile C. Data Filtering ProfileD. Zone Protection Profile Answer: BDExplanation:B: There are two DoS protection mechanisms that the Palo Alto Networks firewalls support.* Flood Protection - Detects and prevents attacks where the network is flooded with packets resulting in too many half-open sessions and/or services being unable to respond to each request. In this case the source address of the attack is usually spoofed.* Resource Protection - Detects and prevent session exhaustion attacks. In this type of attack, a large number of hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources. You can enable both types of protection mechanisms in a single DoS protection profile.D: Provides additional protection between specific network zones in order to protect the zones against attack. The profile must be applied to the entire zone, so it is important to carefully test the profiles in order to prevent issues that may arise with the normal traffic traversing the zones. When defining packets per second (pps) thresholds limits for zone protection profiles, the threshold is based on the packets per second that do not match a previously established session.Incorrect Answers:A: Vulnerability protection stops attempts to exploit system flaws or gain unauthorized access to systems. For example, this feature will protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.C: Data Filtering helps to prevent sensitive information such as credit card or social security numbers from leaving a protected network.
https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/threat-prevention/about-security-profiles QUESTION 22A host attached to Ethernet 1/4 cannot ping the default gateway. The widget on the dashboard shows Ethernet 1/1 and Ethernet 1/4 to be green. The IP address of Ethernet 1/1 is 192.168.1.7 and the IP address of Ethernet 1/4 is 10.1.1.7. The default gateway is attached to Ethernet 1/1. A default route is properly configured.What can be the cause of this problem? A. No Zone has been configured on Ethernet 1/4.B. Interface Ethernet 1/1 is in Virtual Wire Mode.C. DNS has not been properly configured on the firewall.D. DNS has not been properly configured on the host. Answer: A QUESTION 23A VPN connection is set up between Site-A and Site-B, but no traffic is passing in the system log of Site-A, there is an event logged as like-nego-p1-fail-psk.What action will bring the VPN up and allow traffic to start passing between the sites? A. Change the Site-B IKE Gateway profile version to match Site-A,B. Change the Site-A IKE Gateway profile exchange mode to aggressive mode.C. Enable NAT Traversal on the Site-A IKE Gateway profile.D. Change the pre-shared key of Site-B to match the pre-shared key of Site-A Answer: D QUESTION 24A firewall administrator is troubleshooting problems with traffic passing through the Palo Alto Networks firewall. Which method shows the global counters associated with the traffic after configuring the appropriate packet filters? A. From the CLI, issue the show counter global filter pcap yes command.B. From the CLI, issue the show counter global filter packet-filter yes command.C. From the GUI, select show global counters under the monitor tab.D. From the CLI, issue the show counter interface command for the ingress interface. Answer: BExplanation:You can check global counters for a specific source and destination IP addresses by setting a packet filter. We recommend that you use the global counter command with a packet filter to get specific traffic outputs. These outputs will help isolate the issue between two peers.Use the following CLI command to show when traffic is passing through the Palo Alto Networks firewall from that source to destination. > show counter global filter packet-filter yes delta yes Global counters:Elapsed time since last sampling: 20.220 secondsname value rate severity category aspect description
----------pkt_recv 6387398 4 info packet pktproc Packets received
pkt_recv_zero 370391 0 info packet pktproc Packets received from QoS 0Etc.
https://live.paloaltonetworks.com/t5/Management-Articles/How-to-check-global-counters-for-a-specific-source-and/ta-p/65794 QUESTION 25A network security engineer has been asked to analyze Wildfire activity. However, the Wildfire Submissions item is not visible form the Monitor tab.What could cause this condition? A. The firewall does not have an active WildFire subscription.B. The engineer's account does not have permission to view WildFire Submissions.C. A policy is blocking WildFire Submission traffic.D. Though WildFire is working, there are currently no WildFire Submissions log entries. Answer: AExplanation:Native integration with all Palo Alto Networks products allows WildFire to inform and update subscribers with new protective capabilities for the network, cloud and endpoint in real time.
https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/wildfire QUESTION 26Which Palo Alto Networks

VM-Series firewall is supported for VMware NSX? A. VM-100B. VM-200C. VM-1000-HVD. VM-300 Answer: C Explanation:Licenses for the VM-Series NSX Edition FirewallIn order to automate the provisioning and licensing of the VM-Series NSX Edition firewall in the VMware integrated NSX solution, two license bundles are available:One bundle includes the VM-Series capacity license (VM-1000-HV only), Threat Prevention license and a premium support entitlement.Another bundle includes the VM-Series capacity license (VM-1000-HV only) with the complete suite of licenses that include Threat Prevention, GlobalProtect, WildFire, PAN-DB URL Filtering, and a premium support entitlement.
https://www.paloaltonetworks.com/documentation/70/virtualization/virtualization/about-the-vm-series-firewall/license-types-vm-series-firewalls.html QUESTION 27A client is deploying a pair of PA-5000 series firewalls using High Availability (HA) in Active/Passive mode. Which statement is true about this deployment? A. The two devices must share a routable floating IP address B. The two devices may be different models within the PA-5000 seriesC. The HA1 IP address from each peer must be on a different subnetD. The management port may be used for a backup control connection Answer: DExplanation:Set up the backup control link connection.1. In Device > High Availability > General, edit the Control Link (HA1 Backup) section.2. Select the HA1 backup interface and set the IPv4/IPv6 Address and Netmask.Note: Use the management port for the HA1 link.
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/high-availability/configure-active-passive-ha QUESTION 28 What must be used in Security Policy Rule that contain addresses where NAT policy applies? A. Pre-NAT addresse and Pre-NAT zonesB. Post-NAT addresse and Post-Nat zonesC. Pre-NAT addresse and Post-Nat zonesD. Post-Nat addresses and Pre-NAT zones Answer: CExplanation:NAT Policy Rule FunctionalityUpon ingress, the firewall inspects the packet and does a route lookup to determine the egress interface and zone. Then the firewall determines if the packet matches one of the NAT rules that have been defined, based on source and/or destination zone. It then evaluates and applies any security policies that match the packet based on the original (pre-NAT) source and destination addresses, but the post-NAT zones.
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-policy-rules QUESTION 29A company has a policy that denies all applications it classifies as bad and permits only application it classifies as good. The firewall administrator created the following security policy on the company's firewall. Which interface configuration will accept specific VLAN IDs? Which two benefits are gained from having both rule 2 and rule 3 presents? (choose two) A. A report can be created that identifies unclassified traffic on the network.B. Different security profiles can be applied to traffic matching rules 2 and 3.C. Rule 2 and 3 apply to traffic on different ports.D. Separate Log Forwarding profiles can be applied to rules 2 and 3. Answer: AD QUESTION 30How are IPV6 DNS queries configured to user interface ethernet1/3? A. Network > Virtual Router > DNS InterfaceB. Objects > CustomerObjects > DNSC. Network > Interface MgrntD. Device > Setup > Services > Service Route Configuration Answer: DExplanation:Configure the service routes.1. Select Device > Setup > Services > Global and click Service Route Configuration. Note: For the purposes of activating your licenses and getting the most recent content and software updates, you will want to change the service route for DNS, Palo Alto Updates, URL Updates, WildFire, and AutoFocus.2. Click the Customize radio button, and select one of the following:For a predefined service, select IPv4 or IPv6 and click the link for the service for which you want to modify the Source Interface and select the interface you just configured.
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/set-up-network-access-for-external-services
!!!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