[January 2018 Updated Lead2pass Palo Alto Networks PCNSE7 Braindump Free Download 226q

100% Free Lead2pass PCNSE7 New Questions Download: https://www.lead2pass.com/pcnse7.html QUESTION 1A company.com wants to enable Application Override. Given the following screenshot:Which two statements are true if Source and Destination traffic match the Application Override policy? (Choose two)

A. Traffic that matches "rtp-base" will bypass the App-ID and Content-ID engines.B. Traffic will be forced to operate over UDP Port 16384.C. Traffic utilizing UDP Port 16384 will now be identified as "rtp-base".D. Traffic utilizing UDP Port 16384 will bypass the App-ID and Content-ID engines. Answer: CDExplanation:An application override policy is changes how the Palo Alto Networks firewall classifies network traffic into applications. An application override with a custom application prevents the session from being processed by the App-ID engine, which is a Layer-7 inspection. https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Create-an-Application-Override-Policy/ta-p/60044 QUESTION 2Which three fields can be included in a pcap filter? (Choose three) A. Egress interfaceB. Source IPC. Rule numberD. Destination IPE. Ingress interface Answer: BDE QUESTION 3What are three possible verdicts that WildFire can provide for an analyzed sample? (Choose three) A. CleanB. BenginC. AdwareD. SuspiciousE. GraywareF. Malware Answer: BEF Explanation:The WildFire verdicts are: Benign, Grayware, Malware. https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/monitoring/log-severity-levels-and-wildfire-verdicts QUESTION 4A logging infrastructure may need to handle more than 10,000 logs per second.Which two options support a dedicated log collector function? (Choose two) A. Panorama virtual appliance on ESX(i) onlyB. M-500C. M-100 with Panorama installedD. M-100 Answer: BD QUESTION 5What are three valid method of user mapping? (Choose three) A. SyslogB. XML APIC. 802.1XD. WildFireE. Server Monitoring Answer: ABE QUESTION 6A host attached to ethernet1/3 cannot access the internet. The default gateway is attached to ethernet1/4. After troubleshooting. It is determined that traffic cannot pass from the ethernet1/3 to ethernet1/4. What can be the cause of the problem? A. DHCP has been set to Auto.B. Interface ethernet1/3 is in Layer 2 mode and interface ethernet1/4 is in Layer 3 mode.C. Interface ethernet1/3 and ethernet1/4 are in Virtual Wire Mode.D. DNS has not been properly configured on the firewall Answer: BExplanation:In a Layer 2 deployment, the firewall provides switching between two or more interfaces. Each group of interfaces must be assigned to a VLAN object in order for the firewall to switch between them.In a Layer 3 deployment, the firewall routes traffic between ports. An IP address must be assigned to each interface and a virtual router must be defined to route the traffic. Choose this option when routing is required. https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/getting-started/basic-interface-deployments QUESTION 7The IT department has received complaints abou VoIP call jitter when the sales staff is making or receiving calls. QoS is enabled on all firewall interfaces, but there is no QoS policy written in the rulebase. The IT manager wants to find out what traffic is causing the jitter in real time when a user reports the jitter.Which feature can be used to identify, in real time, the applications taking up the most bandwidth? A. QoS StatisticsB. Applications ReportC. Application Command Center (ACC)D. QoS Log Answer: A QUESTION 8A network security engineer is asked to provide a report on bandwidth usage. Which tab in the ACC provides the information needed to create the report? A. Blocked ActivityB. Bandwidth ActivityC. Threat ActivityD. Network Activity Answer: DExplanation:The Network Activity tab of the Application Command Center (ACC) displays an overview of traffic and user activity on your network including:Top applications in useTop users who generate traffic (with a drill down into the bytes, content, threats or URLs accessed by the user)Most used security rules against which traffic matches occurIn addition, you can also view network activity by source or destination zone, region, or IP address, ingress or egress interfaces, and GlobalProtect host information such as the operating systems of the devices most commonly used on the network.

https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/monitoring/acc-tabs.html QUESTION 9Which three options does the WF-500 appliance support for local analysis? (Choose three) A. E-mail linksB. APK filesC. jar filesD. PNG filesE. Portable Executable (PE) files Answer: ACE QUESTION 10Company.com has an in-house application that the Palo Alto Networks device doesn't identify correctly. A Threat Management Team member has mentioned that this in-house application is very sensitive and all traffic being identified needs to be inspected by the Content-ID engine.Which method should company.com use to immediately address this traffic on a Palo Alto Networks device? A. Create a custom Application without signatures, then create an Application Override policy that includes the source, Destination, Destination Port/Protocol and Custom Application of the traffic.B. Wait until an official Application signature is provided from Palo Alto Networks.C. Modify the session timer settings on the closest referanced application to meet the needs of the in-house applicationD. Create a Custom Application with signatures matching unique identifiers of the in-house application traffic Answer: D **PCNSE7 dumps full version (PDF&VCE):** https://www.lead2pass.com/pcnse7.html **Large amount of free PCNSE7 exam questions on Google Drive:** https://drive.google.com/open?id=0B3Syig5i8gpDc3F3eHZRclVhZ3c