[March 2018 Lead2pass 2018 New PCNSE7 Exam PDF Ensure PCNSE7 Certification Exam Pass 100% 226q

Lead2pass 2018 New PCNSE7 Exam PDF Ensure PCNSE7 Certification Exam Pass Successfully:
https://www.lead2pass.com/pcnse7.html QUESTION 11After pushing a security policy from Panorama to a PA-3020 firewall, the firewall administrator notices that traffic logs from the PA-3020 are not appearing in Panorama's traffic logs. What could be the problem? A. A Server Profile has not been configured for logging to this Panorama device.B. Panorama is not licensed to receive logs from this particular firewall.C. The firewall is not licensed for logging to this Panorama device.D. None of the firewall's policies have been assigned a Log Forwarding profileAnswer: D QUESTION 12A critical US-CERT notification is published regarding a newly discovered botnet. The malware is very evasive and is not reliably detected by endpoint antivirus software. Furthermore, SSL is used to tunnel malicious traffic to command-and-control servers on the internet and SSL Forward Proxy Decryption is not enabled.Which component once enabled on a perimeter firewall will allow the identification of existing infected hosts in an environment? A. Anti-Spyware profiles applied outbound security policies with DNS Query action set to sinkholeB. File Blocking profiles applied to outbound security policies with action set to alertC. Vulnerability Protection profiles applied to outbound security policies with action set to blockD. Antivirus profiles applied to outbound security policies with action set to alert Answer: AExplanation:Starting with PAN-OS 6.0, DNS sinkhole is an action that can be enabled in Anti-Spyware profiles. A DNS sinkhole can be used to identify infected hosts on a protected network using DNS traffic in environments where the firewall can see the DNS query to a malicious URL.The DNS sinkhole enables the Palo Alto Networks device to forge a response to a DNS query for a known malicious domain/URL and causes the malicious domain name to resolve to a definable IP address (fake IP) that is given to the client. If the client attempts to access the fake IP address and there is a security rule in place that blocks traffic to this IP, the information is recorded in the logs.
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Configure-DNS-Sinkhole/ta-p/58891 QUESTION 13Which two statements are correct for the out-of-box configuration for Palo Alto Networks NGFWs? (Choose two) A. The devices are pre-configured with a virtual wire pair out the first two interfaces.B. The devices are licensed and ready for deployment.C. The management interface has an IP address of 192.168.1.1 and allows SSH and HTTPS connections.D. A default bidirectional rule is configured that allows Untrust zone traffic to go to the Trust zone.E. The interfaces are pingable. Answer: ACExplanation:
https://popravak.wordpress.com/2014/07/31/initial-setup-of-palo-alto-networks-next-generation-firewall/ QUESTION 14A network security engineer is asked to perform a Return Merchandise Authorization (RMA) on a firewallWhich part of files needs to be imported back into the replacement firewall that is using Panorama? A. Device state and license filesB. Configuration and serial number filesC. Configuration and statistics filesD. Configuration and Large Scale VPN (LSVPN) setups file Answer: A QUESTION 15A network engineer has revived a report of problems reaching 98.139.183.24 through vr1 on the firewall. The routing table on this firewall is extensive and complex.Which CLI command will help identify the issue? A. test routing fib virtual-router vr1B. show routing route type static destination 98.139.183.24C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1D. show routing interface Answer: CExplanation:This document explains how to perform a fib lookup for a particular destination within a particular virtual router on a Palo Alto Networks firewall.1. Select the desired virtual router from the list of virtual routers configured with the command:> test routing fib-lookup virtual-router <value>2. Specify a destination IP address:> test routing fib-lookup virtual-router default ip <ip address>
https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Perform-FIB-Lookup-for-a-Particular-Destination/ta-p/52188 QUESTION 16Which two mechanisms help prevent a spilt brain scenario an Active/Passive High Availability (HA) pair? (Choose two) A. Configure the management interface as HA3 BackupB. Configure Ethernet 1/1 as HA1 BackupC. Configure Ethernet 1/1 as HA2 BackupD. Configure the management interface as HA2 BackupE. Configure the management interface as HA1 BackupF. Configure ethernet1/1 as HA3 Backup Answer: BEExplanation:E: For firewalls without dedicated HA ports, select two data interfaces for the HA2 link and the backup HA1 link. Then, use an Ethernet cable to connect these in-band HA interfaces across both firewalls.Use the management port for the HA1 link and ensure that the management ports can connect to each other across your network.B: 1. In Device > High Availability > General, edit the Control Link (HA1) section.2. Select the interface that you have cabled for use as the HA1 link in the Port drop down menu. Set the IP address and netmask. Enter a Gateway IP address only if the HA1 interfaces are on separate subnets. Do not add a gateway if the devices are directly connected.
https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/high-availability/configure-active-passive-ha QUESTION 17What are three valid actions in a File Blocking Profile? (Choose three) A. ForwardB. BlockC. AlretD. UploadE. Reset-bothF. Continue Answer: BCFExplanation:You can configure a file blocking profile with the following actions:Forward -

When the specified file type is detected, the file is sent to WildFire for analysis. A log is also generated in the data filtering log.Block - When the specified file type is detected, the file is blocked and a customizable block page is presented to the user. A log is also generated in the data filtering log.Alert - When the specified file type is detected, a log is generated in the data filtering log.Continue - When the specified file type is detected, a customizable response page is presented to the user. The user can click through the page to download the file. A log is also generated in the data filtering log. Because this type of forwarding action requires user interaction, it is only applicable for web traffic.Continue-and-forward - When the specified file type is detected, a customizable continuation page is presented to the user. The user can click through the page to download the file. If the user clicks through the continue page to download the file, the file is sent to WildFire for analysis. A log is also generated in the data filtering log.https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/policy/file-blocking-profiles.html QUESTION 18An Administrator is configuring an IPSec VPN toa Cisco ASA at the administrator's home and experiencing issues completing the connection. The following is th output from the command:

```
less mp-log ikemgr.log:

2014-08-05 03:51:41 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:51:41 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <==
2014-08-05 03:52:33 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
timeout.
2014-08-05 03:52:33 [INFO]: ====> PHASE-1 SA DELETED <====
====> Deleted SA: 69.15.96.53[500]-108.81.64.59[500] cookie:09e85260f28f4e15:0000000000000000 <====
2014-08-05 03:53:02 [INFO]: IPsec-SA request for 108.81.64.59 queued since no phase1 found
2014-08-05 03:53:02 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION STARTED AS INITIATOR, MAIN MODE <====
====> Initiated SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <==
2014-08-05 03:53:54 [PROTO_NOTIFY]: ====> PHASE-1 NEGOTIATION FAILED AS INITIATOR, MAIN MODE <====
====> Failed.SA: 69.15.96.53[500]-108.81.64.59[500] cookie:53351420a9a1aa47:0000000000000000 <====
timeout.
2014-08-05 03:53:54 [INFO]: ====> PHASE-1 SA DELETED <====
```


What could be the cause of this problem? A. The public IP addresses do not match for both the Palo Alto Networks Firewall and the ASA.B. The Proxy IDs on the Palo Alto Networks Firewall do not match the settings on the ASA.C. The shared secrets do not match between the Palo Alto firewall and the ASAD. The deed peer detection settings do not match between the Palo Alto Networks Firewall and the ASA Answer: BExplanation:The Proxy IDs could have been checked for mismatch.References: https://live.paloaltonetworks.com/t5/Configuration-Articles/IPSec-Error-IKE-Phase-1-Negotiation-is-Failed-as-Initiator-Main/ta-p/59532 QUESTION 19Which interface configuration will accept specific VLAN IDs? A. Tab ModeB. SubinterfaceC. Access InterfaceD. Trunk Interface Answer: BExplanation:You can only assign a single VLAN to a subinterface, and not to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic.
http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/intrface.html QUESTION 20Palo Alto Networks maintains a dynamic database of malicious domains.Which two Security Platform components use this database to prevent threats? (Choose two) A. Brute-force signaturesB. BrightCloud Url FilteringC. PAN-DB URL FilteringD. DNS-based command-and-control signatures Answer: CDExplanation:C: PAN-DB categorizes URLs based on their content at the domain, file and page level, and receives updates from WildFire cloud-based malware analysis environment every 30 minutes to make sure that, when web content changes, so do categorizations. This continuous feedback loop enables you to keep pace with the rapidly changing nature of the web, automatically.D: DNS is a very necessary and ubiquitous application, as such, it is a very commonly abused protocol for command-and-control and data exfiltration. This tech brief summarizes the DNS classification, inspection and protection capabilities supported by our next-generation security platform, which includes:1. Malformed DNS messages (symptomatic of vulnerability exploitation attack).2. DNS responses with suspicious composition (abused query types, DNS-based denial of service attacks).3. DNS queries for known malicious domains. Our ability to prevent threats from hiding within DNSThe passive DNS network feature allows you to opt-in to share anonymized DNS query and response data with our global passive DNS network. The data is continuously mined to discover malicious domains that are then added to the PAN-OS DNS signature set that is delivered daily, enabling timely detection of compromised hosts within the network and the disruption of command-and-control channels that rely on name resolution.
https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/url-filtering-pandb
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/dns-protection **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