[4/July/2018 Updated Free PassLeader 417q 156-215.80 VCE Braindump with Free PDF Study Guide (Part A)

New Updated 156-215.80 Exam Questions from PassLeader 156-215.80 PDF dumps! Welcome to download the newest PassLeader 156-215.80 VCE dumps: https://www.passleader.com/156-215-80.html (417 Q&As) Keywords: 156-215.80 exam dumps, 156-215.80 exam questions, 156-215.80 VCE dumps, 156-215.80 PDF dumps, 156-215.80 practice tests, 156-215.80 study guide, 156-215.80 braindumps, Check Point Certified Security Administrator (CCSA) R80 Exam P.S. New 156-215.80 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpdm81T0hOX1ZpWGs NEW QUESTION 284 Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except? A.   Create new dashboards to manage 3rd party task. B.   Create products that use and enhance 3rd party solutions. C.   Execute automated scripts to perform common tasks. D.   Create products that use and enhance the Check Point Solution. Answer: A NEW QUESTION 285 In what way are SSL VPN and IPSec VPN different? A.   SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless. B.   SSL VPN adds an extra VPN header to the packet, IPSec VPN does not. C.   IPSec VPN does not support two factor authentication, SSL VPN does support this. D.   IPSec VPN uses an additional virtual adapter, SSL VPN uses the client network adapter only. Answer: D NEW QUESTION 286 Which command can you use to enable or disable multi-queue per interface? A.   cpmq set B.   Cpmqueue set C.   Cpmq config D.   Set cpmq enable Answer: A NEW QUESTION 287 Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue? A.   There is no traffic queue to be handled. B.   Several NICs can use one traffic queue by one CPU. C.   Each NIC has several traffic queues that are handled by multiple CPU cores. D.   Each NIC has one traffic queue that is handled by one CPU. Answer: C NEW QUESTION 288 To fully enable Dynamic Dispatcher on a Security Gateway, you should do what? A.   Run fw ctl multik set_mode 9 in Expert mode and then reboot. B.   Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu. C.   Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot. D.   Run fw ctl multik set_mode 1 in Expert mode and then reboot. Answer: A NEW QUESTION 289 What are types of Check Point APIs available currently as part of R80.10 code? A.   Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API B.   Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API C.   OSE API, OPSEC SDK API, Threat Prevention API and Policy Editor API D.   CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API Answer: B NEW QUESTION 290 What is the purpose of Priority Delta in VRRP? A.   When a box is up, Effective Priority = Priority + Priority Delta. B.   When an Interface is up, Effective Priority = Priority + Priority Delta. C.   When an Interface fails, Effective Priority = Priority - Priority Delta. D.   When a box fails, Effective Priority = Priority - Priority Delta. Answer: C NEW QUESTION 291 The Firewall kernel is replicated multiple times, therefore ____. A.   The Firewall kernel only touches the packet if the connection is accelerated. B.   The Firewall can run different policies per core. C.   The Firewall kernel is replicated only with new connections and deletes itself once the connection times out. D.   The Firewall can run the same policy on all cores. Answer: D NEW QUESTION 292 There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct? A.   Using Web Services B.   Using Mgmt_cli tool C.   Using CLISH D.   Using SmartConsole GUI console Answer: C NEW QUESTION 293 Which the following type of authentication on Mobile Access can NOT be used as the first authentication method? A.   Dynamic ID B.   RADIUS C.   Username and Password D.   Certificate Answer: A NEW QUESTION 294 Which command can you use to verify the number of active concurrent connections? A.   fw conn all B.   fw ctl pst pstat C.   show all connections D.   show connections Answer: B NEW QUESTION 295 Which remote Access Solution is clientless? A.   Checkpoint Mobile B.   Endpoint Security Suite C.   SecuRemote D.   Mobile Access Portal Answer: D NEW QUESTION 296 What component of R80 Management is used for indexing? A.   DBSync B.   API Server C.   fwm D.   SOLR Answer: D NEW

QUESTION 297 Which NAT rules are prioritized first? A.   Post-Automatic/Manual NAT rules B.   Manual/Pre-Automatic NAT C.   Automatic Hide NAT D.   Automatic Static NAT Answer: B NEW QUESTION 298 What is the difference between an event and a log? A.   Events are generated at gateway according to Event Policy. B.   A log entry becomes an event when it matches any rule defined in Event Policy. C.   Events are collected with SmartWorkflow from Trouble Ticket systems. D.   Logs and Events are synonyms. Answer: B NEW QUESTION 299 The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated? A.   There is a virus found. Traffic is still allowed but not accelerated. B.   The connection required a Security server. C.   Acceleration is not enabled. D.   The traffic is originating from the gateway itself. Answer: D NEW QUESTION 300 During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are ____. A.   dropped without sending a negative acknowledgment B.   dropped without logs and without sending a negative acknowledgment C.   dropped with negative acknowledgment D.   dropped with logs and without sending a negative acknowledgment Answer: D NEW QUESTION 301 Which one of the following is true about Threat Extraction? A.   Always delivers a file to user. B.   Works on all MS Office, Executables, and PDF files. C.   Can take up to 3 minutes to complete. D.   Delivers file only if no threats found. Answer: B NEW QUESTION 302 Which is the correct order of a log flow processed by SmartEvent components? A.   Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client B.   Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client C.   Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client D.   Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client Answer: D NEW QUESTION 303 Which of the following statements describes the Check Point ThreatCloud? A.   Blocks or limits usage of web applications. B.   Prevents or controls access to web sites based on category. C.   Prevents Cloud vulnerability exploits. D.   A worldwide collaborative security network. Answer: D NEW QUESTION 304 Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection? A.   Source Address B.   Destination Address C.   TCP Acknowledgment Number D.   Source Port Answer: C NEW QUESTION 305 When defining QoS global properties, which option below is not valid? A.   Weight B.   Authenticated timeout C.   Schedule D.   Rate Answer: C NEW QUESTION 306 The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them? A.   Six times per day B.   Seven times per day C.   Every two hours D.   Every three hours Answer: D NEW QUESTION 307 How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway? A.   Install appliance TE250X on SpanPort on LAN switch in MTA mode. B.   Install appliance TE250X in standalone mode and setup MTA. C.   You can utilize only Check Point Cloud Services for this scenario. D.   It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance. Answer: C NEW QUESTION 308 In SmartEvent, what are the different types of automatic reactions that the administrator can configure? A.   Mail, Block Source, Block Event Activity, External Script, SNMP Trap. B.   Mail, Block Source, Block Destination, Block Services, SNMP Trap. C.   Mail, Block Source, Block Destination, External Script, SNMP Trap. D.   Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap. Answer: A NEW QUESTION 309 Identify the API that is not supported by Check Point currently. A.   R80 Management API B.   Identity Awareness Web Services API C.   Open REST API D.   OPSEC SDK Answer: C NEW QUESTION 310 Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI? A.   mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt B.   mgmt_cli add host name "Server_1" ip_address "10.15.123.10" --format json C.   mgmt_cli add object-host "Server_1" ip_address "10.15.123.10" --format json D.   mgmt_cli add object "Server_1" ip_address "10.15.123.10" --format json Answer: A NEW QUESTION 311 SandBlast has several functional components that work together to ensure that

attacks are prevented in real-time. Which the following is NOT part of the SandBlast component? A.   Threat Emulation B.   Mobile Access C.   Mail Transfer Agent D.   Threat Cloud Answer: C NEW QUESTION 312 Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway? A.   SandBlast Threat Emulation B.   SandBlast Agent C.   Check Point Protect D.   SandBlast Threat Extraction Answer: D NEW QUESTION 313 What is the command to see cluster status in cli expert mode? A.   fw ctl stat B.   clusterXL stat C.   clusterXL status D.   cphaprob stat Answer: A NEW QUESTION 314 On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port ____. A.   18210 B.   18184 C.   257 D.   18191 Answer: B NEW QUESTION 315 If the first packet of an UDP session is rejected by a security policy, what does the firewall send to the client? A.   Nothing B.   TCP FIN C.   TCP RST D.   ICMP unreachable Answer: A NEW QUESTION 316 What is the mechanism behind Threat Extraction? A.   This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender. B.   This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient. C.   This is a new mechanism to identify the IP address of the sender of malicious codes and to put it into the SAM database (Suspicious Activity Monitoring). D.   Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast. Answer: D NEW QUESTION 317 What is the benefit of Manual NAT over Automatic NAT? A.   If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy. B.   There is no benefit since Automatic NAT has in any case higher priority over Manual NAT. C.   You have the full control about the priority of the NAT rules. D.   On IPSO and GAIA Gateways, it is handled in a Stateful manner. Answer: C NEW QUESTION 318 The CPD daemon is a Firewall Kernel Process that does NOT do which of the following? A.   Secure Internal Communication (SIC) B.   Restart Daemons if they fail C.   Transfer messages between Firewall processes D.   Pulls application monitoring status Answer: D NEW QUESTION 319 Which of the following is NOT an attribute of packer acceleration? A.   Source address B.   Protocol C.   Destination port D.   Application Awareness Answer: D NEW QUESTION 320 Which is a suitable command to check whether Drop Templates are activated or not? A.   fw ctl get int activate_drop_templates B.   fwaccel stat C.   fwaccel stats D.   fw ctl templates Answer: B NEW QUESTION 321 Please choose correct command syntax to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI. A.   host name myHost12 ip-address 10.50.23.90 B.   mgmt add host name ip-address 10.50.23.90 C.   add host name emailserver1 ip-address 10.50.23.90 D.   mgmt add host name emailserver1 ip-address 10.50.23.90 Answer: D NEW QUESTION 322 The CDT utility supports which of the following? A.   Major version upgrades to R77.30 B.   Only Jumbo HFA's and hotfixes C.   Only major version upgrades to R80.10 D.   All upgrades Answer: D NEW QUESTION 323 Using ClusterXL, what statement is true about the Sticky Decision Function? A.   Can only be changed for Load Sharing implementations. B.   All connections are processed and synchronized by the pivot. C.   Is configured using cpconfig. D.   Is only relevant when using SecureXL. Answer: A NEW QUESTION 324 What command would show the API server status? A.   cpm status B.   api restart C.   api status D.   show api status Answer: D NEW QUESTION 325 How Capsule Connect and Capsule Workspace differ? A.   Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications. B.   Capsule Workspace can provide access to any application. C.   Capsule Connect provides Business data isolation. D.   Capsule Connect does not require an installed application at client. Answer: A NEW QUESTION 326 Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older? A.   The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are

defined, allowing control over the rule base flow and which security functionalities take precedence. B.   Limits the upload and download throughput for streaming media in the company to 1 Gbps. C.   Time object to a rule to make the rule active only during specified times. D.   Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule. Answer: D NEW QUESTION 327 What are the three components for Check Point Capsule? A.   Capsule Docs, Capsule Cloud, Capsule Connect B.   Capsule Workspace, Capsule Cloud, Capsule Connect C.   Capsule Workspace, Capsule Docs, Capsule Connect D.   Capsule Workspace, Capsule Docs, Capsule Cloud Answer: D NEW QUESTION 328 Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this? A.   UDP port 265 B.   TCP port 265 C.   UDP port 256 D.   TCP port 256 Answer: B NEW QUESTION 329 What is true about the IPS-Blade? A.   In R80, IPS is managed by the Threat Prevention Policy. B.   In R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict. C.   In R80, IPS Exceptions cannot be attached to "all rules". D.   In R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same. Answer: A NEW QUESTION 330 Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks? A.   Go to clash-Run cpstop | Run cpstart. B.   Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway. C.   Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores. D.   Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy. Answer: B NEW QUESTION 331 When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition? A.   Any size. B.   Less than 20 GB. C.   More than 10 GB and less than 20 GB. D.   At least 20 GB. Answer: D NEW QUESTION 332 Which firewall daemon is responsible for the FW CLI commands? A.   fwd B.   fwm C.   cpm D.   cpd Answer: A NEW QUESTION 333 If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of the following steps should NOT be performed? A.   Rename the hostname of the Standby member to match exactly the hostname of the Active member. B.   Change the Standby Security Management Server to Active. C.   Change the Active Security Management Server to Standby. D.   Manually synchronize the Active and Standby Security Management Servers. Answer: A NEW QUESTION 334 Using R80 Smart Console, what does a "pencil icon" in a rule mean? A.   I have changed this rule. B.   Someone else has changed this rule. C.   This rule is managed by check point's SOC. D.   This rule can't be changed as it's an implied rule. Answer: A NEW QUESTION 335 Which method below is NOT one of the ways to communicate using the Management API's? A.   Typing API commands using the "mgmt_cli" command. B.   Typing API commands from a dialog box inside the SmartConsole GUI application. C.   Typing API commands using Gaia's secure shell (clash) 19+. D.   Sending API commands over an http connection using web-services. Answer: D NEW QUESTION 336 Session unique identifiers are passed to the web api using which http header option? A.   X-chkp-sid B.   Accept-Charset C.   Proxy-Authorization D.   Application Answer: C NEW QUESTION 337 What is the main difference between Threat Extraction and Threat Emulation? A.   Threat Emulation never delivers a file and takes more than 3 minutes to complete. B.   Threat Extraction always delivers a file and takes less than a second to complete. C.   Threat Emulation never delivers a file that takes less than a second to complete. D.   Threat Extraction never delivers a file and takes more than 3 minutes to complete. Answer: B NEW QUESTION 338 Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade? A.   Detects and blocks malware by correlating multiple detection engines before users are affected. B.   Configure rules to limit the available network bandwidth for specified users or groups. C.   Use UserCheck to help users understand that certain websites are against the company's security policy. D.   Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels. Answer: A NEW QUESTION 339 You want to store the GAiA configuration in a file for later reference. What command

should you use? A.   write mem <filename> B.   show config -f <filename> C.   save config -o <filename> D.   save configuration <filename> Answer: D NEW QUESTION 340 Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic? A.   Slow Path B.   Medium Path C.   Fast Path D.   Accelerated Path Answer: A NEW QUESTION 341 From SecureXL perspective, what are the tree paths of traffic flow? A.   Initial Path; Medium Path; Accelerated Path B.   Layer Path; Blade Path; Rule Path C.   Firewall Path; Accept Path; Drop Path D.   Firewall Path; Accelerated Path; Medium Path Answer: D NEW QUESTION 342 You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server? A.   fwd B.   fwm C.   cpd D.   cpwd Answer: B NEW QUESTION 343 R80.10 management server can manage gateways with which versions installed? A.   Versions R77 and higher B.   Versions R76 and higher C.   Versions R75.20 and higher D.   Version R75 and higher Answer: B NEW QUESTION 344 You want to verify if there are unsaved changes in GAiA that will be lost with a reboot. What command can be used? A.   show unsaved B.   show save-state C.   show configuration diff D.   show config-state Answer: D NEW QUESTION 345 In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway? A.   SND is a feature to accelerate multiple SSL VPN connections. B.   SND is an alternative to IPSec Main Mode, using only 3 packets. C.   SND is used to distribute packets among Firewall instances. D.   SND is a feature of fw monitor to capture accelerated packets. Answer: C NEW QUESTION 346 Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster. A.   Symmetric routing B.   Failovers C.   Asymmetric routing D.   Anti-Spoofing Answer: B NEW QUESTION 347 What are the steps to configure the HTTPS Inspection Policy? A.   Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard B.   Go to Application&url filtering blade > Advanced > Https Inspection > Policy C.   Go to Manage&Settings > Blades > HTTPS Inspection > Policy D.   Go to Application&url filtering blade > Https Inspection > Policy Answer: C NEW QUESTION 348 What is the difference between SSL VPN and IPSec VPN? A.   IPSec VPN does not require installation of a resident VPN client. B.   SSL VPN requires installation of a resident VPN client. C.   SSL VPN and IPSec VPN are the same. D.   IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser. Answer: D NEW QUESTION 349 Which statement is NOT TRUE about Delta synchronization? A.   Using UDP Multicast or Broadcast on port 8161. B.   Using UDP Multicast or Broadcast on port 8116. C.   Quicker than Full sync. D.   Transfers changes in the Kernel tables between cluster members. Answer: A NEW QUESTION 350 Under which file is the proxy arp configuration stored? A. $FWDIR/state/proxy_arp.conf on the management server B. $FWDIR/conf/local.arp on the management server C. $FWDIR/state/_tmp/proxy.arp on the security gateway D. $FWDIR/conf/local.arp on the gateway Answer: D Download the newest PassLeader 156-215.80 dumps from passleader.com now! 100% Pass Guarantee! 156-215.80 PDF dumps & 156-215.80 VCE dumps: https://www.passleader.com/156-215-80.html (417 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New 156-215.80 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpdm81T0hOX1ZpWGs