[20/June/2018 Updated Reliable PassLeader 156-915.80 Braindump with VCE and PDF Dumps Free Download (Part B)

New Updated 156-915.80 Exam Questions from PassLeader 156-915.80 PDF dumps! Welcome to download the newest PassLeader 156-915.80 VCE dumps: https://www.passleader.com/156-915-80.html (365 Q&As)

Keywords: 156-915.80 exam dumps, 156-915.80 exam questions, 156-915.80 VCE dumps, 156-915.80 PDF dumps, 156-915.80 practice tests, 156-915.80 study guide, 156-915.80 braindumps, Check Point Certified Security Expert Update - R80 Exam

P.S. New 156-915.80 dumps PDF: https://drive.google.com/open?id=1HMGEPKVBag2Bm5dUy2POfhbnpk-1-vCT

NEW QUESTION 316

What GUI client would you use to view an IPS packet capture?

A.   SmartView Monitor
B.   SmartView Tracker
C.   Smart Update
D.   Smart Reporter

Answer: B

NEW QUESTION 317

What is the valid range for VRID value in VRRP configuration?

A.   1-254
B.   1-255
C.   0-254
D.   0-255

Answer: B

NEW QUESTION 318

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 319

Which command will reset the kernel debug options to default settings?

A.   fw ctl dbg -a 0
B.   fw ctl dbg resetall
C.   fw ctl debug 0
D.   fw ctl debug set 0

Answer: C

NEW QUESTION 320

You need to change the number of firewall instances used by CoreXL. How can you achieve this goal?

A.   edit fwaffinity.conf; reboot required
B.   cpconfig; reboot required
C.   edit fwaffinity.conf; reboot not required
D.   cpconfig, reboot not required

Answer: B

NEW QUESTION 321

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A.   That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
B.   Full Layer4 VPN -SSL VPN that gives users network access to all mobile applications.

C.   Full layer3 VPN -IPSec VPN that gives users network access to all mobile applications.

D.   You can make sure that documents are sent to the intended recipients only.

Answer: C

NEW QUESTION 322

What does the following command do?

vpn crl_zap

A.   Nothing, it is not a valid command.

B.   Erases all CRLs from the gateway cache.

C.   Erases VPN certificates from cache.

D.   Erases CRLs from the management server cache.

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/12467.htm

NEW QUESTION 323

Firewall policies must be configured to accept VRRP packets on the GAiA platform if it runs Firewall software. The Multicast destination assigned by the Internet Assigned Numbers Authority (IANA) for VRRP is ____.

A.   224.0.0.18

B.   224.0.0.5

C.   224.0.0.102

D.   224.0.0.22

Answer: A

NEW QUESTION 324

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: D

NEW QUESTION 325

GAiA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the ____.

A.   Check Point Upgrade Service Engine

B.   Check Point Software Update Agent

C.   Check Point Remote Installation Daemon (CPRID)

D.   Check Point Software Update Daemon

Answer: A

NEW QUESTION 326

Which one of following is NOT a firewall chain?

A.   RTM packet in (rtm)

B.   VPN node add (vpnad)

C.   IP Options restore (in) (ipopt_res)

D.   Fw SCV inbound (scv)

Answer: B

NEW QUESTION 327

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 -d

Answer: B

NEW QUESTION 328

Which directory below contains log files?

A.   /opt/CPSmartlog-R80/log

B.   /opt/CPshrd-R80/log

C.   /opt/CPsuite-R80/fw1/log

D.   /opt/CPsuite-R80/log

Answer: C

NEW QUESTION 329

What is the responsibility of SOLR process on R80.10 management server?

A.   Validating all data before it's written into the database.

B.   It generates indexes of data written to the database.

C.   Communication between SmartConsole applications and the Security Management Server.

D.   Writing all information into the database.

Answer: B

NEW QUESTION 330

VPN Tunnel Sharing can be configured with any of the options below, EXCEPT ____.

A.   Gateway-based

B.   Subnet-based

C.   IP range based

D.   Host-based

Answer: C

NEW QUESTION 331

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 332

What can you do to see the current number of kernel instances in a system with CoreXL enabled?

A.   Browse to Secure Platform Web GUI

B.   Only Check Point support personnel can access that information

C.   Execute SmarDashboard client

D.   Execute command cpconfig

Answer: D

NEW QUESTION 333

When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of ___.

A.   Threat Emulation

B.   HTTPS

C.   QOS

D.   VolP

Answer: D

NEW QUESTION 334

Why would you not see a CoreXL configuration option in cpconfig?

A.   The gateway only has one processor.

B.   CoreXL is not licenses.

C.   CoreXL is disabled via policy.

D.   CoreXL is not enabled in the gateway object.

Answer: A

NEW QUESTION 335

In SPLAT the command to set the timeout was idle. In order to achieve this and increase the timeout for Gaia, what command do you use?

A.   set

idle <value>

B.   set

inactivity-timeout <value>

C.   set

timeout <value>

D.   set

inactivity <value>

Answer: B

NEW QUESTION 336

What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

A.   Anti-Bot is the only countermeasure against unknown malware.

B.   Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers.

C.   Anti-Bot is the only signature-based method of malware protection.

D.   Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.

Answer: D

NEW QUESTION 337

SmartEvent does NOT use which of the following procedures to identify events?

A.   Matching a log against each event definition

B.   Create an event candidate

C.   Matching a log against local exclusions

D.   Matching a log against global exclusions

Answer: C

NEW QUESTION 338

In Gaia, if one is unsure about a possible command, what command lists all possible commands?

A.   show all grep commands

B.   show configuration

C.   show commands

D.   get all commands

Answer: C

NEW QUESTION 339

In which case is a Sticky Decision Function relevant?

A.   Load Sharing - Multicast

B.   Load Balancing - Forward

C.   High Availability

D.   Load Sharing - Unicast

Answer: C

NEW QUESTION 340

The Security Gateway is installed on GAiA R80. The default port for the Web User Interface is _____.

A.   TCP 18211

B.   TCP 257

C.   TCP 4433

D.   TCP 443

Answer: D

NEW QUESTION 341

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point

architecture component?

A.   None, Security Management Server would be installed by itself.
B.   SmartConsole.
C.   SecureClient.
D.   SmartEvent.

Answer: D

NEW QUESTION 342

The tool ____ generates a R80 Security Gateway configuration report.

A.   infoCP
B.   infoview
C.   cpinfo
D.   fw cpinfo

Answer: C

NEW QUESTION 343

The R80 utility fw is used to troubleshoot ____.

A.   user data base corruption
B.   EDAP conflicts
C.   traffic issues
D.   phase two key negotiation

Answer: C

NEW QUESTION 344

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

A.   Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
B.   Create a separate Security Policy package for each remote Security Gateway.
C.   Create network objects that restrict all applicable rules to only certain networks.
D.   Run separate SmartConsole instances to login and configure each security Gateway directly.

Answer: B

NEW QUESTION 345

Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will be need if he does NOT include a SmartConsole machine in his calculations?

A.   One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
B.   One machine.
C.   Two machines.
D.   Three machines.

Answer: C

NEW QUESTION 346

The command ____ provides the most complete restoration of a R80 configuration.

A.   upgrade_import
B.   cpconfig
C.   fwn dbimport -p <export file>
D.   cpinfo -recover

Answer: A

NEW QUESTION 347

Which of the following statements is TRUE about R80 management plug-ins?

A.   The plug-in is a package installed on the Security Gateway.
B.   Installing a management plug-in requires a Snapshot, just like any upgrade process.
C.   A management plug-in interacts with a Security Management Server to provide new features and support for new products.
D.   Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Answer: C

NEW QUESTION 348

The R80 feature _____ permits blocking specific IP addresses for a specified time period.

A.   Block Port Overflow

B.   Local Interface Spoofing

C.   Suspicious Activity Monitoring

D.   Adaptive Threat Prevention

Answer: C

NEW QUESTION 349

In R80 spoofing is defined as a method of: _____.

A.   Disguising an illegal IP address behind an authorized IP address through Port Address Translation

B.   Hiding your firewall from unauthorized users

C.   Detecting people using false or wrong authentication logins

D.   Making packets appear as if they come from an authorized IP address

Answer: D

NEW QUESTION 350

Which features are only supported with R80.10 Gateways but not R77.x?

A.   Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access
Software Blade policies.

B.   Limits the upload and download throughput for streaming media in the company to 1 Gbps.

C.   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.

D.   Time object to a rule to make the rule active only during specified times.

Answer: C

NEW QUESTION 351

For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

A.   20 minutes

B.   15 minutes

C.   Admin account cannot be unlocked automatically

D.   30 minutes at least

Answer: D

NEW QUESTION 352

What scenario indicates that SecureXL is enabled?

A.   Dynamic objects are available in the Object Explorer

B.   SecureXL can be disabled in cpconfig

C.   fwaccel commands can be used in clish

D.   Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 353

What is the command to show SecureXL status?

A.   fwaccel status

B.   fwaccel stats -m

C.   fwaccel -s

D.   fwaccel stat

Answer: D

NEW QUESTION 354

Which web services protocol is used to communicate to the Check Point R80 identity Awareness Web APi?

A.   SOAP

B.   REST

C.   XLANG

D.   XML-RPC

Answer: B

NEW QUESTION 355

Which file gives you a list of all security servers in use, including port number?

A. $FWDIR/conf/conf.conf
B. $FWDIR/conf/servers.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/conf/serversd.conf

Answer: C

NEW QUESTION 356

What CLI command will reset the IPS pattern matcher statistics?

A.   ips reset pmstat
B.   ips pstats reset
C.   ips pmstats refresh
D.   ips pmstats reset

Answer: D

NEW QUESTION 357

GAiA Software update packages can be imported and installed offline in situation where ____.

A.   Security Gateway with GAiA does NOT have SFTP access to Internet
B.   Security Gateway with GAiA does NOT have access to Internet
C.   Security Gateway with GAiA does NOT have SSH access to internet
D.   The desired CPUSE package is ONLY available in the Check Point CLOUD

Answer: B

NEW QUESTION 358

The Event List within the Events tab contains ____.

A.   a list of options available for running a query
B.   the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list
C.   events generated by a query
D.   the details of a selected event

Answer: C

NEW QUESTION 359

What is mandatory for ClusterXL to work properly?

A.   The number of cores must be the same on every participating cluster node.
B.   The Magic MAC number must be unique per cluster node.
C.   The Sync Interface must not have an IP address configured.
D.   If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on all cluster members.

Answer: B

NEW QUESTION 360

Which one of the following processes below would not start if there was a licensing issue?

A.   CPD
B.   CPCA
C.   FWM
D.   CPWD

Answer: A

NEW QUESTION 361

Aaron is a Cyber Security Engineer working for Global Law Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R80.10. Company's Network Security Developer Team is having issue testing new API with newly deployed R80.10 Security Management Server and blames Check Point Security Management Server as root cause. The ticket has been created and issue is at Aaron's desk for an investigation. What do you recommend as the best suggestion for Aaron to make sure API testing works as expected?

A.   Aaron should check API Server status from expert CLI by "fwm api status" and if it's stopped he should start using command "fwm api start" on Security Management Server.

B.   Aaron should check API Server status from expert CLI by "cpapi status" and if it's stopped he should start using command "cpapi start" on Security Management Server.

C.   Aaron should check API Server status from expert CLI by "api status" and if it's stopped he should start using command "api start" on Security Management Server.

D.   Aaron should check API Server status from expert CLI by "cpm api status" and if it's stopped he should start using command "cpm api start" on Security Management Server.

Answer: C

NEW QUESTION 362

What utility would you use to configure route-based VPNs?

A.   vpn
shell

B.   vpn
tu

C.   vpn sw_topology

D.   vpn
set_slim_server

Answer: A

NEW QUESTION 363

Where do you create and modify the Mobile Access policy in R80?

A.   SmartConsole

B.   SmartMonitor

C.   SmartEndpoint

D.   SmartDashboard

Answer: A

NEW QUESTION 364

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

A.   Export R80 configuration, clean install R80.10 and import the configuration.

B.   CPUSE online upgrade.

C.   CPUSE offline upgrade.

D.   SmartUpdate upgrade.

Answer: C

NEW QUESTION 365

What is the port used for SmartConsole to connect to the Security Management Server?

A.   CPMI port 18191/TCP

B.   CPM port / TCP port 19009

C.   SIC port 18191/TCP

D.   https port 4434/TCP

Answer: A

P.S. New 156-915.80 dumps PDF: https://drive.google.com/open?id=1HMGEPKVBag2Bm5dUy2POfhbnpk-1-vCT