

Exam Questions 156-315.80

Check Point Certified Security Expert - R80

<https://www.2passeasy.com/dumps/156-315.80/>



NEW QUESTION 1

What happen when IPS profile is set in Detect Only Mode for troubleshooting?

- A. It will generate Geo-Protection traffic
- B. Automatically uploads debugging logs to Check Point Support Center
- C. It will not block malicious traffic
- D. Bypass licenses requirement for Geo-Protection control

Answer: C

Explanation:

It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic.

During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION 2

Which of the following is NOT a component of Check Point Capsule?

- A. Capsule Docs
- B. Capsule Cloud
- C. Capsule Enterprise
- D. Capsule Workspace

Answer: C

NEW QUESTION 3

To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?

- A. 5 Network; Host; Objects; Services; API
- B. 3 Incoming; Outgoing; Network
- C. 2 Internal; External
- D. 4 Incoming; Outgoing; Internal; Other

Answer: D

NEW QUESTION 4

What is a best practice before starting to troubleshoot using the “fw monitor” tool?

- A. Run the command: fw monitor debug on
- B. Clear the connections table
- C. Disable CoreXL
- D. Disable SecureXL

Answer: D

NEW QUESTION 5

John detected high load on sync interface. Which is most recommended solution?

- A. For short connections like http service – delay sync for 2 seconds
- B. Add a second interface to handle sync traffic
- C. For short connections like http service – do not sync
- D. For short connections like icmp service – delay sync for 2 seconds

Answer: A

NEW QUESTION 6

What is not a purpose of the deployment of Check Point API?

- A. Execute an automated script to perform common tasks
- B. Create a customized GUI Client for manipulating the objects database
- C. Create products that use and enhance the Check Point solution
- D. Integrate Check Point products with 3rd party solution

Answer: B

NEW QUESTION 7

The Check Point history feature in R80 provides the following:

- A. View install changes and install specific version
- B. View install changes
- C. Policy Installation Date, view install changes and install specific version
- D. Policy Installation Date only

Answer: C

NEW QUESTION 8

Which of the following is NOT a VPN routing option available in a star community?

- A. To satellites through center only.
- B. To center, or through the center to other satellites, to Internet and other VPN targets.
- C. To center and to other satellites through center.
- D. To center only.

Answer: AD

NEW QUESTION 9

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 10

What is the name of the secure application for Mail/Calendar for mobile devices?

- A. Capsule Workspace
- B. Capsule Mail
- C. Capsule VPN
- D. Secure Workspace

Answer: A

NEW QUESTION 10

What command would show the API server status?

- A. cpm status
- B. api restart
- C. api status
- D. show api status

Answer: C

NEW QUESTION 14

What are the two high availability modes?

- A. Load Sharing and Legacy
- B. Traditional and New
- C. Active and Standby
- D. New and Legacy

Answer: D

Explanation:

ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION 17

Which component is NOT required to communicate with the Web Services API?

- A. API key
- B. session ID token
- C. content-type
- D. Request payload

Answer: A

NEW QUESTION 20

Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is _____. .

- A. Sent to the Internal Certificate Authority.
- B. Sent to the Security Administrator.
- C. Stored on the Security Management Server.
- D. Stored on the Certificate Revocation List.

Answer: D

NEW QUESTION 22

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 27

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 32

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

- A. logd
- B. fwd
- C. fwm
- D. cpd

Answer: B

NEW QUESTION 34

To add a file to the Threat Prevention Whitelist, what two items are needed?

- A. File name and Gateway
- B. Object Name and MD5 signature
- C. MD5 signature and Gateway
- D. IP address of Management Server and Gateway

Answer: B

NEW QUESTION 36

To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

- A. fw ctl Dyn_Dispatch on
- B. fw ctl Dyn_Dispatch enable
- C. fw ctl multik set_mode 4
- D. fw ctl multik set_mode 1

Answer: C

NEW QUESTION 39

What is the command to show SecureXL status?

- A. fwaccel status
- B. fwaccel stats -m
- C. fwaccel -s
- D. fwaccel stat

Answer: D

Explanation:

To check overall SecureXL status: [Expert@HostName]# fwaccel stat References:

NEW QUESTION 41

What can we infer about the recent changes made to the Rule Base?

- A. Rule 7 was created by the 'admin' administrator in the current session
- B. 8 changes have been made by administrators since the last policy installation
- C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
- D. Rule 1 and object webserver are locked by another administrator

Answer: D

NEW QUESTION 42

Which TCP-port does CPM process listen to?

- A. 18191
- B. 18190
- C. 8983
- D. 19009

Answer: D

NEW QUESTION 44

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

- A. Limit
- B. Resource
- C. Custom Application / Site
- D. Network Object

Answer: B

NEW QUESTION 45

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. Fill 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 50

SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

- A. This statement is true because SecureXL does improve all traffic.
- B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
- C. This statement is true because SecureXL does improve this traffic.
- D. This statement is false because encrypted traffic cannot be inspected.

Answer: C

Explanation:

SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

NEW QUESTION 54

Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?

- A. /opt/CPshrd-R80/conf/local.arp
- B. /var/opt/CPshrd-R80/conf/local.arp
- C. \$CPDIR/conf/local.arp
- D. \$FWDIR/conf/local.arp

Answer: D

NEW QUESTION 57

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 61

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 62

John is using Management HA. Which Smartcenter should be connected to for making changes?

- A. secondary Smartcenter
- B. active Smartcenter
- C. connect virtual IP of Smartcenter HA
- D. primary Smartcenter

Answer: B

NEW QUESTION 65

Fill in the blank: The "fw monitor" tool can be best used to troubleshoot _____.

- A. AV issues
- B. VPN errors
- C. Network issues
- D. Authentication issues

Answer: C

NEW QUESTION 67

What is the SandBlast Agent designed to do?

- A. Performs OS-level sandboxing for SandBlast Cloud architecture
- B. Ensure the Check Point SandBlast services is running on the end user's system
- C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network
- D. Clean up email sent with malicious attachments

Answer: C

NEW QUESTION 72

Fill in the blank: Identity Awareness AD-Query is using the Microsoft _____ API to learn users from AD.

- A. WMI
- B. Eventvwr
- C. XML
- D. Services.msc

Answer: A

NEW QUESTION 73

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. Security Gateway
- E. SmartEvent

Answer: D

NEW QUESTION 76

Fill in the blank: Authentication rules are defined for _____.

- A. User groups
- B. Users using UserCheck
- C. Individual users
- D. All users in the database

Answer: A

NEW QUESTION 78

What component of R80 Management is used for indexing?

- A. DBSync
- B. API Server

- C. fwm
- D. SOLR

Answer: D

NEW QUESTION 81

True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.

- A. True, CLI is the prefer method for Licensing
- B. False, Central License are handled via Security Management Server
- C. False, Central Licenses are installed via Gaia on Security Gateways
- D. True, Central License can be installed with CPLIC command on a Security Gateway

Answer: D

NEW QUESTION 84

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

- A. Check Point Remote User
- B. Check Point Capsule Workspace
- C. Check Point Mobile Web Portal
- D. Check Point Capsule Remote

Answer: C

NEW QUESTION 86

Why would an administrator see the message below?

- A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 91

Which command would disable a Cluster Member permanently?

- A. clusterXL_admin down
- B. cphaprob_admin down
- C. clusterXL_admin down-p
- D. set clusterXL down-p

Answer: C

NEW QUESTION 95

Check Point security components are divided into the following components:

- A. GUI Client, Security Gateway, WebUI Interface
- B. GUI Client, Security Management, Security Gateway
- C. Security Gateway, WebUI Interface, Consolidated Security Logs
- D. Security Management, Security Gateway, Consolidate Security Logs

Answer: B

NEW QUESTION 96

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 100

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

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 105

SmartEvent uses it's event policy to identify events. How can this be customized?

- A. By modifying the firewall rulebase
- B. By creating event candidates
- C. By matching logs against exclusions
- D. By matching logs against event rules

Answer: C

NEW QUESTION 109

Which options are given on features, when editing a Role on Gaia Platform?

- A. Read/Write, Read Only
- B. Read/Write, Read Only, None
- C. Read/Write, None
- D. Read Only, None

Answer: B

NEW QUESTION 114

When using CPSTAT, what is the default port used by the AMON server?

- A. 18191
- B. 18192
- C. 18194
- D. 18190

Answer: B

NEW QUESTION 116

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment.

Which details she need to fill in System Restore window before she can click OK button and test the backup?

- A. Server, SCP, Username, Password, Path, Comment, Member
- B. Server, TFTP, Username, Password, Path, Comment, All Members
- C. Server, Protocol, Username, Password, Path, Comment, All Members
- D. Server, Protocol, username Password, Path, Comment, Member

Answer: C

NEW QUESTION 117

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

- A. Right click Accept in the rule, select “More”, and then check ‘Enable Identity Captive Portal’.
- B. On the firewall object, Legacy Authentication screen, check ‘Enable Identity Captive Portal’.
- C. In the Captive Portal screen of Global Properties, check ‘Enable Identity Captive Portal’.
- D. On the Security Management Server object, check the box ‘Identity Logging’.

Answer: A

NEW QUESTION 122

Which Check Point software blade provides Application Security and identity control?

- A. Identity Awareness
- B. Data Loss Prevention
- C. URL Filtering
- D. Application Control

Answer: D

NEW QUESTION 124

Which of the following process pulls application monitoring status?

- A. fwd
- B. fwm
- C. cpwd
- D. cpd

Answer: D

NEW QUESTION 129

Which of the following is NOT an alert option?

- A. SNMP
- B. High alert
- C. Mail
- D. User defined alert

Answer: B

NEW QUESTION 131

With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

- A. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
- B. For end users to access the native applications, they need to install the SSL Network Extender.
- C. HTTPS for web-based applications and AES or RSA algorithm for native application
- D. For end users to access the native application, they need to install the SSL Network Extender.
- E. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
- F. For end users to access the native applications, no additional software is required.
- G. HTTPS for web-based applications and AES or RSA algorithm for native application
- H. For end users to access the native application, no additional software is required.

Answer: A

NEW QUESTION 135

What SmartEvent component creates events?

- A. Consolidation Policy
- B. Correlation Unit
- C. SmartEvent Policy
- D. SmartEvent GUI

Answer: B

NEW QUESTION 140

What does the Log "Views" tab show when SmartEvent is Correlating events?

- A. A list of common reports
- B. Reports for customization
- C. Top events with charts and graphs
- D. Details of a selected logs

Answer: C

NEW QUESTION 144

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

Explanation:

Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:

- Matching a Log Against Global Exclusions
- Matching a Log Against Each Event Definition
- Creating an Event Candidate
- When a Candidate Becomes an Event References:

NEW QUESTION 149

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 153

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

- A. Security Gateway IP-address cannot be changed without re-establishing the trust.
- B. The Security Gateway name cannot be changed in command line without re-establishing trust.
- C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust.
- D. The Security Management Server IP-address cannot be changed without re-establishing the trust.

Answer: A

NEW QUESTION 157

When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

- A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
- B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
- C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
- D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

Answer: D

NEW QUESTION 162

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated management console. It empowers the migration from legacy Client-side logic to Server-side logic. The cpm process:

- A. Allow GUI Client and management server to communicate via TCP Port 19001
- B. Allow GUI Client and management server to communicate via TCP Port 18191
- C. Performs database tasks such as creating, deleting, and modifying objects and compiling policy.
- D. Performs database tasks such as creating, deleting, and modifying objects and compiling as well as policy code generation.

Answer: C

NEW QUESTION 164

When setting up an externally managed log server, what is one item that will not be configured on the R80 Security Management Server?

- A. IP
- B. SIC
- C. NAT
- D. FQDN

Answer: C

NEW QUESTION 165

How long may verification of one file take for Sandblast Threat Emulation?

- A. up to 1 minutes
- B. within seconds cleaned file will be provided
- C. up to 5 minutes
- D. up to 3 minutes

Answer: B

NEW QUESTION 170

Which command will allow you to see the interface status?

- A. cphaprob interface
- B. cphaprob -l interface
- C. cphaprob -a if
- D. cphaprob stat

Answer: C

NEW QUESTION 175

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 rule
- B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- D. Time object to a rule to make the rule active only during specified times.
- E. Sub Policies are sets of rules that can be created and attached to specific rule
- F. 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 177

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new 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
- D. Check Point will make use of the newly installed CPU and Cores
- E. 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 179

You find one of your cluster gateways showing "Down" when you run the "cphaprob stat" command. You then run the "clusterXL_admin up" on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

- A. cphaprob -f register
- B. cphaprob -d -s report
- C. cpstat -f all
- D. cphaprob -a list

Answer: D

NEW QUESTION 180

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

Answer: B

NEW QUESTION 183

In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Stateful Mode configuration, chain modules marked with _____ will not apply.

- A. ffff
- B. 1
- C. 3
- D. 2

Answer: D

NEW QUESTION 185

VPN Link Selection will perform the following when the primary VPN link goes down?

- A. The Firewall will drop the packets.
- B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
- C. The Firewall will send out the packet on all interfaces.

D. The Firewall will inform the client that the tunnel is down.

Answer: B

NEW QUESTION 189

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 192

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 197

When simulating a problem on ClusterXL cluster with `cphaprob -d STOP -s problem -t 0 register`, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

- A. `cphaprob -d STOP unregister`
- B. `cphaprob STOP unregister`
- C. `cphaprob unregister STOP`
- D. `cphaprob -d unregister STOP`

Answer: A

Explanation:

esting a failover in a controlled manner using following command;
`cphaprob -d STOP -s problem -t 0 register`
This will register a problem state on the cluster member this was entered on; If you then run;
`cphaprob list`
this will show an entry named STOP.
to remove this problematic register run following;
`cphaprob -d STOP unregister` References:

NEW QUESTION 200

An administrator would like to troubleshoot why templating is not working for some traffic. How can he determine at which rule templating is disabled?

- A. He can use the `fw accel stat` command on the gateway.
- B. He can use the `fw accel statistics` command on the gateway.
- C. He can use the `fwaccel stat` command on the Security Management Server.
- D. He can use the `fwaccel stat` command on the gateway

Answer: D

NEW QUESTION 204

In which formats can Threat Emulation forensics reports be viewed in?

- A. TXT, XML and CSV
- B. PDF and TXT
- C. PDF, HTML, and XML
- D. PDF and HTML

Answer: C

NEW QUESTION 208

Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

- A. 15 sec
- B. 60 sec
- C. 5 sec
- D. 30 sec

Answer: B

NEW QUESTION 212

Which tool is used to enable ClusterXL?

- A. SmartUpdate
- B. cpconfig
- C. SmartConsole
- D. sysconfig

Answer: B

NEW QUESTION 213

The Firewall Administrator is required to create 100 new host objects with different IP addresses. What API command can he use in the script to achieve the requirement?

- A. add host name <New HostName> ip-address <ip address>
- B. add hostname <New HostName> ip-address <ip address>
- C. set host name <New HostName> ip-address <ip address>
- D. set hostname <New HostName> ip-address <ip address>

Answer: A

NEW QUESTION 218

Which is not a blade option when configuring SmartEvent?

- A. Correlation Unit
- B. SmartEvent Unit
- C. SmartEvent Server
- D. Log Server

Answer: B

Explanation:

On the Management tab, enable these Software Blades: References:

NEW QUESTION 221

What API command below creates a new host with the name “New Host” and IP address of “192.168.0.10”?

- A. new host name “New Host” ip-address “192.168.0.10”
- B. set host name “New Host” ip-address “192.168.0.10”
- C. create host name “New Host” ip-address “192.168.0.10”
- D. add host name “New Host” ip-address “192.168.0.10”

Answer: D

NEW QUESTION 222

What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?

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

Answer: B

NEW QUESTION 224

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

NEW QUESTION 226

Which command collects diagnostic data for analyzing customer setup remotely?

- A. cpinfo
- B. migrate export
- C. sysinfo
- D. cpview

Answer: A

Explanation:

CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

NEW QUESTION 231

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

Answer: B

NEW QUESTION 234

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(clish)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 236

Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

- A. You can assign only one profile per gateway and a profile can be assigned to one rule Only.
- B. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.
- C. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.
- D. You can assign only one profile per gateway and a profile can be assigned to one or more rules.

Answer: C

NEW QUESTION 238

If you needed the Multicast MAC address of a cluster, what command would you run?

- A. cphaprob -a if
- B. cphaconf ccp multicast
- C. cphaconf debug data
- D. cphaprob igmp

Answer: D

NEW QUESTION 243

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT
- B. IP pool NAT, static NAT, hide NAT
- C. Static NAT, automatic NAT, hide NAT
- D. Static NAT, hide NAT, IP pool NAT

Answer: A

NEW QUESTION 246

What Factor preclude Secure XL Templating?

- A. Source Port Ranges/Encrypted Connections
- B. IPS
- C. ClusterXL in load sharing Mode
- D. CoreXL

Answer: A

NEW QUESTION 249

Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

- A. Synchronized
- B. Never been synchronized
- C. Lagging
- D. Collision

Answer: D

NEW QUESTION 253

You have a Gateway is running with 2 cores. You plan to add a second gateway to build a cluster and used a device with 4 cores. How many cores can be used in a Cluster for Firewall-kernel on the new device?

- A. 3
- B. 2
- C. 1
- D. 4

Answer: D

NEW QUESTION 256

What is the Implicit Clean-up Rule?

- A. A setting is defined in the Global Properties for all policies.
- B. A setting that is configured per Policy Layer.
- C. Another name for the Clean-up Rule.
- D. Automatically created when the Clean-up Rule is defined.

Answer: C

NEW QUESTION 258

When installing a dedicated R80 SmartEvent server. What is the recommended size of the root partition?

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20GB
- D. At least 20GB

Answer: D

NEW QUESTION 262

Security Checkup Summary can be easily conducted within:

- A. Summary
- B. Views
- C. Reports
- D. Checkups

Answer: B

NEW QUESTION 265

What is not a component of Check Point SandBlast?

- A. Threat Emulation
- B. Threat Simulator
- C. Threat Extraction
- D. Threat Cloud

Answer: B

NEW QUESTION 268

Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Firewall
- B. Threat Emulation
- C. Application Control
- D. Threat Extraction

Answer: B

NEW QUESTION 270

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

Explanation:

On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

NEW QUESTION 272

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 offline upgrade
- C. CPUSE online upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 277

Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to manager?

- A. fw accel stat
- B. fwaccel stat
- C. fw acces stats
- D. fwaccel stats

Answer: B

NEW QUESTION 280

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _____ .

- A. TCP port 19009
- B. TCP Port 18190
- C. TCP Port 18191
- D. TCP Port 18209

Answer: A

NEW QUESTION 285

Which command shows detailed information about VPN tunnels?

- A. cat \$FWDIR/conf/vpn.conf
- B. vpn tu tlist
- C. vpn tu
- D. cpview

Answer: B

NEW QUESTION 290

How do Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications.
- C. Capsule Workspace can provide access to any application.
- D. Capsule Connect provides Business data isolation.
- E. Capsule Connect does not require an installed application at client.

Answer: A

NEW QUESTION 292

You have existing dbedit scripts from R77. Can you use them with R80.10?

- A. dbedit is not supported in R80.10
- B. dbedit is fully supported in R80.10
- C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
- D. dbedit scripts are being replaced by mgmt_cli in R80.10

Answer: D

NEW QUESTION 295

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-315.80 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-315.80 Product From:

<https://www.2passeasy.com/dumps/156-315.80/>

Money Back Guarantee

156-315.80 Practice Exam Features:

- * 156-315.80 Questions and Answers Updated Frequently
- * 156-315.80 Practice Questions Verified by Expert Senior Certified Staff
- * 156-315.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-315.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year