

## Exam Questions 156-315.80

Check Point Certified Security Expert - R80

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



#### NEW QUESTION 1

Which of the SecureXL templates are enabled by default on Security Gateway?

- A. Accept
- B. Drop
- C. NAT
- D. None

**Answer:** D

#### NEW QUESTION 2

What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

- A. Use Multi-Domain Management Server.
- B. Choose different setting for log storage and SmartEvent db
- C. Install Management and SmartEvent on different machines.
- D. it is not possible.

**Answer:** B

#### NEW QUESTION 3

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 Wire Mode configuration, chain modules marked with \_\_\_\_\_ will not apply.

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

**Answer:** B

#### NEW QUESTION 4

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 5

In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?

- A. If the Action of the matching rule is Accept the gateway will drop the packet
- B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down
- C. If the Action of the matching rule is Drop the gateway stops matching against later rules in the Policy Rule Base and drops the packet
- D. If the rule does not matched in the Network policy it will continue to other enabled polices

**Answer:** C

#### Explanation:

[https://sc1.checkpoint.com/documents/R80/CP\\_R80\\_SecMGMT/html\\_frameset.htm?topic=documents/R80/CP\\_](https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_)

#### NEW QUESTION 6

Which blades and or features are not supported in R80?

- A. SmartEvent Maps
- B. SmartEvent
- C. Identity Awareness
- D. SmartConsole Toolbars

**Answer:** A

#### NEW QUESTION 7

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 8

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats.
- B. Proactively detects threats.
- C. Delivers file with original content.
- D. Delivers PDF versions of original files with active content removed.

**Answer:** B

#### NEW QUESTION 9

NAT rules are prioritized in which order?

- 1. Automatic Static NAT
- 2. Automatic Hide NAT
- 3. Manual/Pre-Automatic NAT
- 4. Post-Automatic/Manual NAT rules

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

**Answer:** A

#### NEW QUESTION 10

The SmartEvent R80 Web application for real-time event monitoring is called:

- A. SmartView Monitor
- B. SmartEventWeb
- C. There is no Web application for SmartEvent
- D. SmartView

**Answer:** B

#### NEW QUESTION 10

Which command lists all tables in Gaia?

- A. fw tab -t
- B. fw tab -list
- C. fw-tab -s
- D. fw tab -1

**Answer:** C

#### NEW QUESTION 13

What is the minimum amount of RAM needed for a Threat Prevention Appliance?

- A. 6 GB
- B. 8GB with Gaia in 64-bit mode
- C. 4 GB
- D. It depends on the number of software blades enabled

**Answer:** C

#### NEW QUESTION 18

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 19

You need to see which hotfixes are installed on your gateway, which command would you use?

- A. cpinfo -h all
- B. cpinfo -o hotfix
- C. cpinfo -l hotfix
- D. cpinfo -y all

**Answer:** D

#### NEW QUESTION 20

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 22

What are the different command sources that allow you to communicate with the API server?

- A. SmartView Monitor, API\_cli Tool, Gaia CLI, Web Services
- B. SmartConsole GUI Console, mgmt\_cli Tool, Gaia CLI, Web Services
- C. SmartConsole GUI Console, API\_cli Tool, Gaia CLI, Web Services
- D. API\_cli Tool, Gaia CLI, Web Services

**Answer:** B

#### NEW QUESTION 26

SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?

- A. Application and Client Service
- B. Network and Application
- C. Network and Layers
- D. Virtual Adapter and Mobile App

**Answer:** B

#### NEW QUESTION 30

What is true of the API server on R80.10?

- A. By default the API-server is activated and does not have hardware requirements.
- B. By default the API-server is not active and should be activated from the WebUI.
- C. By default the API server is active on management and stand-alone servers with 16GB of RAM (or more).
- D. By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8GB of RAM (or more).

**Answer:** D

#### NEW QUESTION 33

The Event List within the Event 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 37

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 42

In ClusterXL Load Sharing Multicast Mode:

- A. only the primary member received packets sent to the cluster IP address
- B. only the secondary member receives packets sent to the cluster IP address
- C. packets sent to the cluster IP address are distributed equally between all members of the cluster
- D. every member of the cluster received all of the packets sent to the cluster IP address

**Answer:** D

#### NEW QUESTION 45

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
- B. Traffic is still allowed but not accelerated.
- C. The connection required a Security server.
- D. Acceleration is not enabled.
- E. The traffic is originating from the gateway itself.

**Answer:** D

#### NEW QUESTION 49

What must you do first if “fwm sic\_reset” could not be completed?

- A. Cpstop then find keyword “certificate” in objects\_5\_0.C and delete the section
- B. Reinitialize SIC on the security gateway then run “fw unloadlocal”
- C. Reset SIC from Smart Dashboard
- D. Change internal CA via cpconfig

**Answer:** D

#### NEW QUESTION 54

Which one of the following is true about Threat Emulation?

- A. Takes less than a second to complete
- B. Works on MS Office and PDF files only
- C. Always delivers a file
- D. Takes minutes to complete (less than 3 minutes)

**Answer:** D

#### NEW QUESTION 57

When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

**Answer:** A

#### NEW QUESTION 62

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 64

You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

- A. SmartEvent Client Info
- B. SecuRemote
- C. Check Point Protect
- D. Check Point Capsule Cloud

**Answer:** C

#### NEW QUESTION 68

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

- A. CPML port 18191/TCP
- B. CPM port/TCP port 19009
- C. SIC port 18191/TCP
- D. https port 4434/TCP

**Answer:** A

#### NEW QUESTION 73

Which statement is true about ClusterXL?

- A. Supports Dynamic Routing (Unicast and Multicast)
- B. Supports Dynamic Routing (Unicast Only)
- C. Supports Dynamic Routing (Multicast Only)

D. Does not support Dynamic Routing

**Answer:** A

#### NEW QUESTION 76

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. Transfers messages between Firewall processes
- D. Pulls application monitoring status

**Answer:** D

#### NEW QUESTION 77

There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW\_A and FW\_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW\_A is configured to have higher priority than FW\_B. FW\_A was active and processing the traffic in the morning. FW\_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW\_B became active. After an hour, FW\_A's interface issues were resolved and it became operational.

When it re-joins the cluster, will it become active automatically?

- A. No, since 'maintain' current active cluster member' option on the cluster object properties is enabled by default.
- B. No, since 'maintain' current active cluster member' option is enabled by default on the Global Properties.
- C. Yes, since 'Switch to higher priority cluster member' option on the cluster object properties is enabled by default.
- D. Yes, since 'Switch to higher priority cluster member' option is enabled by default on the Global Properties.

**Answer:** A

#### NEW QUESTION 78

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 83

Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

- A. 50%
- B. 75%
- C. 80%
- D. 15%

**Answer:** D

#### NEW QUESTION 87

During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

- A. Host having a Critical event found by Threat Emulation
- B. Host having a Critical event found by IPS
- C. Host having a Critical event found by Antivirus
- D. Host having a Critical event found by Anti-Bot

**Answer:** D

#### NEW QUESTION 91

You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?

- A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH
- B. ifconfig eth1 hw 11:11:11:11:11:11; expert
- C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
- D. ethtool -i eth2 mac 11:11:11:11:11:11; expert

**Answer:** A

#### NEW QUESTION 95

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 96

Which GUI client is supported in R80?

- A. SmartProvisioning
- B. SmartView Tracker
- C. SmartView Monitor
- D. SmartLog

**Answer:** C

#### NEW QUESTION 98

Which TCP-port does CPM process listen to?

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

**Answer:** D

#### NEW QUESTION 103

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 105

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 106

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 107

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

- A. RADIUS
- B. Remote Access and RADIUS
- C. AD Query
- D. AD Query and Browser-based Authentication

**Answer:** D

#### Explanation:

Identity Awareness gets identities from these acquisition sources:

#### NEW QUESTION 109

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 114

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 117

Which command is used to add users to or from existing roles?

- A. Add rba user <User Name> roles <List>
- B. Add rba user <User Name>
- C. Add user <User Name> roles <List>
- D. Add user <User Name>

**Answer:** A

#### NEW QUESTION 122

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 124

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the checkbox to enable pre-shared secret and cannot be enabled.

Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

**Answer:** C

#### NEW QUESTION 128

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. Versions R75 and higher

**Answer:** C

#### NEW QUESTION 132

Fill in the blanks: Gaia can be configured using the \_\_\_\_\_ or \_\_\_\_\_.

- A. GaiaUI; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

**Answer:** C

#### NEW QUESTION 134

Fill in the blanks. There are \_\_\_\_\_ types of software containers: \_\_\_\_\_.

- A. Three; security management, Security Gateway, and endpoint security
- B. Three; Security Gateway, endpoint security, and gateway management



- C. Two; security management and endpoint security
- D. Two; endpoint security and Security Gateway

**Answer:** A

#### NEW QUESTION 136

Please choose the path to monitor the compliance status of the Check Point R80.10 based management.

- A. Gateways & Servers --> Compliance View
- B. Compliance blade not available under R80.10
- C. Logs & Monitor --> New Tab --> Open compliance View
- D. Security & Policies --> New Tab --> Compliance View

**Answer:** C

#### NEW QUESTION 141

How often does Threat Emulation download packages by default?

- A. Once a week
- B. Once an hour
- C. Twice per day
- D. Once per day

**Answer:** D

#### NEW QUESTION 142

You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore\_backup
- B. import backup
- C. cp\_merge
- D. migrate import

**Answer:** D

#### NEW QUESTION 146

Which command shows actual allowed connections in state table?

- A. fw tab -t StateTable
- B. fw tab -t connections
- C. fw tab -t connection
- D. fw tab connections

**Answer:** B

#### NEW QUESTION 147

Which command gives us a perspective of the number of kernel tables?

- A. fw tab -t
- B. fw tab -s
- C. fw tab -n
- D. fw tab -k

**Answer:** B

#### NEW QUESTION 151

How many policy layers do Access Control policy support?

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

**Answer:** A

#### Explanation:

Two policy layers:  
- Network Policy Layer  
- Application Control Policy Layer

#### NEW QUESTION 153

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention

- C. Application Control and URL Filtering
- D. Network and Application Control

**Answer:** D

#### NEW QUESTION 156

What command can you use to have cpinfo display all installed hotfixes?

- A. cpinfo -hf
- B. cpinfo -y all
- C. cpinfo -get hf
- D. cpinfo installed\_jumbo

**Answer:** B

#### NEW QUESTION 158

After the initial installation on Check Point appliance, you notice that the Management-interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
- B. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
- D. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

**Answer:** A

#### NEW QUESTION 162

GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

- A. Check Point Update 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 165

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

- A. Threat Emulation
- B. HTTPS
- C. QOS
- D. VoIP

**Answer:** D

#### NEW QUESTION 167

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 169

You have enabled "Full Log" as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R80 gateways.

**Answer:** A

#### NEW QUESTION 171

Which encryption algorithm is the least secured?

- A. AES-128
- B. AES-256
- C. DES
- D. 3DES

**Answer:** C

#### NEW QUESTION 176

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

#### Explanation:

The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

#### NEW QUESTION 179

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 182

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

#### NEW QUESTION 183

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 184

On what port does the CPM process run?

- A. TCP 857
- B. TCP 18192
- C. TCP 900
- D. TCP 19009

**Answer:** D

#### NEW QUESTION 189

Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when \_\_\_\_\_. .

- A. The license is attached to the wrong Security Gateway.
- B. The existing license expires.
- C. The license is upgraded.
- D. The IP address of the Security Management or Security Gateway has changed.

**Answer:** A

#### NEW QUESTION 190

What key is used to save the current CPView page in a filename format cpview\_”cpview process ID”.cap”number of captures”?

- A. S
- B. W
- C. C
- D. Space bar

**Answer:** C

**NEW QUESTION 194**

Fill in the blank: \_\_\_\_\_ information is included in “Full Log” tracking option, but is not included in “Log” tracking option?

- A. Destination port
- B. Data type
- C. File attributes
- D. Application

**Answer:** B

**NEW QUESTION 195**

SandBlast appliances can be deployed in the following modes:

- A. using a SPAN port to receive a copy of the traffic only
- B. detect only
- C. inline/prevent or detect
- D. as a Mail Transfer Agent and as part of the traffic flow only

**Answer:** C

**NEW QUESTION 196**

Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or \_\_\_\_\_.

- A. On all satellite gateway to satellite gateway tunnels
- B. On specific tunnels for specific gateways
- C. On specific tunnels in the community
- D. On specific satellite gateway to central gateway tunnels

**Answer:** C

**NEW QUESTION 201**

Which of the following is NOT an alert option?

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

**Answer:** B

**NEW QUESTION 202**

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 207**

What command lists all interfaces using Multi-Queue?

- A. cpmq get
- B. show interface all
- C. cpmq set
- D. show multiqueue all

**Answer:** A

**NEW QUESTION 211**

What SmartEvent component creates events?

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

**Answer:** B

**NEW QUESTION 213**

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 218

Which command shows the current connections distributed by CoreXL FW instances?

- A. fw ctl multik stat
- B. fw ctl affinity -l
- C. fw ctl instances -v
- D. fw ctl iflist

**Answer:** A

#### NEW QUESTION 221

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 225

Capsule Connect and Capsule Workspace both offer secured connection for remote users who are using their mobile devices. However, there are differences between the two.

Which of the following statements correctly identify each product's capabilities?

- A. Workspace supports ios operating system, Android, and WP8, whereas Connect supports ios operating system and Android only
- B. For compliance/host checking, Workspace offers the MDM cooperative enforcement, whereas Connectoffers both jailbreak/root detection and MDM cooperative enforcement.
- C. For credential protection, Connect uses One-time Password login support and has no SSO support, whereas Workspace offers both One-Time Password and certain SSO login support.
- D. Workspace can support any application, whereas Connect has a limited number of application types which it will support.

**Answer:** C

#### NEW QUESTION 226

Fill in the blank: The tool \_\_\_\_\_ generates a R80 Security Gateway configuration report.

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

**Answer:** C

#### NEW QUESTION 230

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 232

Which of the following links will take you to the SmartView web application?

- A. <https://<Security Management Server host name>/smartviewweb/>
- B. <https://<Security Management Server IP Address>/smartview/>
- C. <https://<Security Management Server host name>smartviewweb>
- D. <https://<Security Management Server IP Address>/smartview>

**Answer:** B

#### NEW QUESTION 237

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 242

SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data. Which component is NOT part of the SandBlast Mobile solution?

- A. Management Dashboard
- B. Gateway
- C. Personal User Storage
- D. Behavior Risk Engine

**Answer:** C

#### NEW QUESTION 245

In the R80 SmartConsole, on which tab are Permissions and Administrators defined?

- A. Security Policies
- B. Logs and Monitor
- C. Manage and Settings
- D. Gateways and Servers

**Answer:** C

#### NEW QUESTION 248

Which command will allow you to see the interface status?

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

**Answer:** C

#### NEW QUESTION 250

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 252

Which is NOT a SmartEvent component?

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

**Answer:** C

#### NEW QUESTION 257

What is the purpose of the CPCA process?

- A. Monitoring the status of processes.
- B. Sending and receiving logs.
- C. Communication between GUI clients and the SmartCenter server.
- D. Generating and modifying certificates.

**Answer:** D



#### NEW QUESTION 260

What are the methods of SandBlast Threat Emulation deployment?

- A. Cloud, Appliance and Private
- B. Cloud, Appliance and Hybrid
- C. Cloud, Smart-1 and Hybrid
- D. Cloud, OpenServer and Vmware

**Answer:** A

#### NEW QUESTION 261

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 264

To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

- A. fw ctl set int fwha vmac global param enabled
- B. fw ctl get int vmac global param enabled; result of command should return value 1
- C. cphaprob-a if
- D. fw ctl get int fwha\_vmac\_global\_param\_enabled; result of command should return value 1

**Answer:** D

#### NEW QUESTION 265

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

**Answer:** C

#### NEW QUESTION 266

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 269

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

#### NEW QUESTION 270

What is the mechanism behind Threat Extraction?

- A. This 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 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 274

What is the most recommended way to install patches and hotfixes?

- A. CPUSE Check Point Update Service Engine
- B. rpm -Uv
- C. Software Update Service
- D. UnixinstallScript

**Answer:** A

#### NEW QUESTION 276

Which command is used to display status information for various components?

- A. show all systems
- B. show system messages
- C. sysmess all
- D. show sysenv all

**Answer:** D

#### NEW QUESTION 277

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

**Answer:** D

#### NEW QUESTION 280

SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

- A. Analyzes each log entry as it arrives at the log server according to the Event Polic
- B. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.
- C. Correlates all the identified threats with the consolidation policy.
- D. Collects syslog data from third party devices and saves them to the database.
- E. Connects with the SmartEvent Client when generating threat reports.

**Answer:** A

#### NEW QUESTION 283

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 288

Which packet info is ignored with Session Rate Acceleration?

- A. source port ranges
- B. source ip
- C. source port
- D. same info from Packet Acceleration is used

**Answer:** C

#### NEW QUESTION 293

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:** A

#### NEW QUESTION 298

Connections to the Check Point R80 Web API use what protocol?

- A. HTTPS
- B. RPC
- C. VPN

D. SIC

**Answer:** A

#### NEW QUESTION 302

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 306

What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?

- A. 4 Interfaces – an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
- B. 3 Interfaces – an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
- C. 1 Interface – an interface leading to the organization and the Internet, and configure for synchronization.
- D. 2 Interfaces – a data interface leading to the organization and the Internet, a second interface for synchronization.

**Answer:** B

#### NEW QUESTION 309

With SecureXL enabled, accelerated packets will pass through the following:

- A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
- B. Network Interface Card, Check Point Firewall Kernel, and the Acceleration Device
- C. Network Interface Card and the Acceleration Device
- D. Network Interface Card, OSI Network Layer, and the Acceleration Device

**Answer:** C

#### NEW QUESTION 314

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 rule
- D. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- E. Time object to a rule to make the rule active only during specified times.

**Answer:** C

#### NEW QUESTION 318

Which tool is used to enable ClusterXL?

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

**Answer:** B

#### NEW QUESTION 320

fwssd is a child process of which of the following Check Point daemons?

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

**Answer:** A

#### NEW QUESTION 322

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 323

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
- D. Yes, but only one has the right to write.

**Answer:** C

#### NEW QUESTION 325

How is communication between different Check Point components secured in R80? As with all questions, select the BEST answer.

- A. By using IPSEC
- B. By using SIC
- C. By using ICA
- D. By using 3DES

**Answer:** B

#### NEW QUESTION 327

Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.

What will happen to the changes already made?

- A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom will have to reboot his SmartConsole computer, clear to cache, and restore changes.

**Answer:** A

#### NEW QUESTION 328

What information is NOT collected from a Security Gateway in a Cpinfo?

- A. Firewall logs
- B. Configuration and database files
- C. System message logs
- D. OS and network statistics

**Answer:** A

#### NEW QUESTION 332

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 333

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 336

What is the default shell of Gaia CLI?

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

**Answer:** B

**NEW QUESTION 338**

Which utility allows you to configure the DHCP service on Gaia from the command line?

- A. ifconfig
- B. dhcp\_ofg
- C. sysconfig
- D. cpconfig

**Answer:** C

**NEW QUESTION 341**

Which 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 345**

In the Firewall chain mode FFF refers to:

- A. Stateful Packets
- B. No Match
- C. All Packets
- D. Stateless Packets

**Answer:** C

**NEW QUESTION 347**

What are the main stages of a policy installations?

- A. Verification & Compilation, Transfer and Commit
- B. Verification & Compilation, Transfer and Installation
- C. Verification, Commit, Installation
- D. Verification, Compilation & Transfer, Installation

**Answer:** B

**NEW QUESTION 352**

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 356**

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 359**

SandBlast agent extends 0 day prevention to what part of the network?

- A. Web Browsers and user devices
- B. DMZ server
- C. Cloud
- D. Email servers

**Answer:** A

**NEW QUESTION 362**

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 365

Fill in the blank: The R80 utility fw monitor is used to troubleshoot \_\_\_\_\_ .

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiations

**Answer:** C

#### Explanation:

Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

#### NEW QUESTION 367

Both ClusterXL and VRRP are fully supported by Gaia R80.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

- A. cphaprob stat
- B. cphaprob -a if
- C. cphaprob -l list
- D. cphaprob all show stat

**Answer:** D

#### NEW QUESTION 371

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

- A. Smart Cloud Services
- B. Load Sharing Mode Services
- C. Threat Agent Solution
- D. Public Cloud Services

**Answer:** A

#### NEW QUESTION 374

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 enabled which path is handling the traffic?

- A. Slow Path
- B. Medium Path
- C. Fast Path
- D. Accelerated Path

**Answer:** A

#### NEW QUESTION 378

CPM process stores objects, policies, users, administrators, licenses and management data in a database. The database is:

- A. MySQL
- B. Postgres SQL
- C. MarisDB
- D. SOLR

**Answer:** B

#### NEW QUESTION 380

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 381

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 383

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 387

Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and \_\_\_\_\_ consolidate billions of logs and shows them as prioritized security events.

- A. SmartMonitor
- B. SmartView Web Application
- C. SmartReporter
- D. SmartTracker

**Answer:** B

#### NEW QUESTION 390

The following command is used to verify the CPUSE version:

- A. HostName:0>show installer status build
- B. [Expert@HostName:0]#show installer status
- C. [Expert@HostName:0]#show installer status build
- D. HostName:0>show installer build

**Answer:** A

#### NEW QUESTION 392

Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances. Steve's manager, Diana, asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?

- A. fw tab -t connections -s
- B. fw tab -t connections
- C. fw tab -t connections -c
- D. fw tab -t connections -f

**Answer:** B

#### NEW QUESTION 396

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 398

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 400

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 402

What is the benefit of “fw monitor” over “tcpdump”?

- A. “fw monitor” reveals Layer 2 information, while “tcpdump” acts at Layer 3.
- B. “fw monitor” is also available for 64-Bit operating systems.
- C. With “fw monitor”, you can see the inspection points, which cannot be seen in “tcpdump”
- D. “fw monitor” can be used from the CLI of the Management Server to collect information from multiple gateways.

**Answer:** C

#### NEW QUESTION 404

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage Setting
- B. Security Policies
- C. Gateway and Servers
- D. Logs and Monitor

**Answer:** D

#### NEW QUESTION 409

.....

## 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