# Exam Questions 156-315.80

Check Point Certified Security Expert - R80

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

**NEW QUESTION 1**
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 2**
Which of these statements describes the Check Point ThreatCloud?

A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network

**Answer:** D

**NEW QUESTION 3**
After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

A. cvpnd_restart
B. cvpnd_restart
C. cvpnd restart
D. cvpnrestart

**Answer:** B

**NEW QUESTION 4**
To fully enable Dynamic Dispatcher on a Security Gateway:

A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
B. Using cpconfig, update the Dynamic Dispatcher value to “full” under the CoreXL menu.
C. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
D. run fw multik set_mode 1 in Expert mode and then reboot.

**Answer:** A

**NEW QUESTION 5**
Which command can you use to enable or disable multi-queue per interface?

A. cpmq set
B. Cpmqueue set
C. Cpmq config
D. St cpmq enable

**Answer:** A

**NEW QUESTION 6**
Please choose correct command to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90
B. mgmt: add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90
D. mgmt: add host name emailserver1 ip-address 10.50.23.90

**Answer:** D

**NEW QUESTION 7**
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 8**
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 9**
SmartEvent provides a convenient way to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands. They appear only on cells that refer to IP addresses because the IP address of the active cell is used as the destination of the command when run. The default commands are:

A. ping, traceroute, netstat, and route
B. ping, nslookup, Telnet, and route
C. ping, whois, nslookup, and Telnet
D. ping, traceroute, netstat, and nslookup

**Answer:** C

**NEW QUESTION 10**
As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?

A. SFWDIR/smartevent/conf
B. $RTDIR/smartevent/conf
C. $RTDIR/smartview/conf
D. $FWDIR/smartview/conf

**Answer:** C

**NEW QUESTION 10**
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 14**
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

A. Formal; corporate
B. Local; formal
C. Local; central
D. Central; local

**Answer:** D

**NEW QUESTION 19**
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 restricts all applicable rules to only certain networks.
D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

**Answer:** B

**NEW QUESTION 22**
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 25**
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 28**
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 32**
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw ctl multik dynamic_dispatching on
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. fw ctl multik pq enable

**Answer:** C

**NEW QUESTION 36**
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 38**
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 40**
You plan to automate creating new objects using new R80 Management API. You decide to use GAIA CLI for this task.
What is the first step to run management API commands on GAIA's shell?

A. mgmt_admin@teabag > id.txt
B. mgmt_login
C. login user admin password teabag
D. mgmt_cli login user "admin" password "teabag" > id.txt

**Answer:** B

**NEW QUESTION 44**
What is the correct order of the default "fw monitor" inspection points?

A. i, I, o, O
B. 1, 2, 3, 4
C. i, o, I, O
D. I, i, O, o

**Answer:** C

**NEW QUESTION 45**
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 48**
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 51**
Automation and Orchestration differ in that:

A. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
B. Automation involves the process of coordinating an exchange of information through web service interactions such as XML and JSON, but orchestration does not involve processes.
C. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and puts them all together into a process workflow.
D. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.

**Answer:** A

**NEW QUESTION 56**
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 58**
Which of the following is NOT a type of Check Point API available in R80.10?

A. Identity Awareness Web Services
B. OPSEC SDK
C. Mobile Access
D. Management

**Answer:** C

**NEW QUESTION 59**
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 64**
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 65**
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 66**
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 70**
Which GUI client is supported in R80?

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

**Answer:** C

**NEW QUESTION 72**
When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

**Answer:** C

**NEW QUESTION 77**
Which of the following will NOT affect acceleration?

A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)

**Answer:** B

**NEW QUESTION 79**
Which process handles connection from SmartConsole R80?

A. fwm
B. cpmd
C. cpm
D. cpd

**Answer:** C

**NEW QUESTION 84**
What is the correct command to observe the Sync traffic in a VRRP environment?

A. fw monitor –e “accept[12:4,b]=224.0.0.18;”
B. fw monitor –e “accept port(6118;”
C. fw monitor –e “accept proto=mcVRRP;”
D. fw monitor –e “accept dst=224.0.0.18;”

**Answer:** D

**NEW QUESTION 86**
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-m ail. 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 89**

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 93**
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 95**
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 98**
What is the least amount of CPU cores required to enable CoreXL?

A. 2
B. 1
C. 4
D. 6

**Answer:** B

**NEW QUESTION 101**
Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid
B. Accept-Charset
C. Proxy-Authorization
D. Application

**Answer:** C

**NEW QUESTION 102**
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 106**
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 109**
Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R80.
What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R80?

A. Missing an installed R77.20 Add-on on Security Management Server
B. Unsupported firmware on UTM-1 Edge-W appliance
C. Unsupported version on UTM-1 570 series appliance
D. Unsupported appliances on remote locations

**Answer:** A

**NEW QUESTION 114**
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 116**
True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

A. False, this feature has to be enabled in the Global Properties.
B. True, every administrator works in a session that is independent of the other administrators.
C. True, every administrator works on a different database that is independent of the other administrators.
D. False, only one administrator can login with write permission.

**Answer:** B

**NEW QUESTION 117**
What component of R80 Management is used for indexing?

A. DBSync
B. API Server
C. fwm
D. SOLR

**Answer:** D

**NEW QUESTION 120**
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

A. cphaprob set int fwha_vmac_global_param_enabled 1
B. clusterXL set int fwha_vmac_global_param_enabled 1
C. fw ctl set int fwha_vmac_global_param_enabled 1
D. cphaconf set int fwha_vmac_global_param_enabled 1

**Answer:** C

**NEW QUESTION 123**
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

A. Threat Emulation
B. Mobile Access
C. Mail Transfer Agent
D. Threat Cloud

**Answer:** C

**NEW QUESTION 127**
Which statement is most correct regarding about “CoreXL Dynamic Dispatcher”?

A. The CoreXL FW instances assignment mechanism is based on Source MAC addresses, Destination MAC addresses
B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
C. The CoreXL FW instances assignment mechanism is based on IP Protocol type
D. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP ‘Protocol’ type

**Answer:** B

**NEW QUESTION 131**
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 132**
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 133**
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 137**
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 139**
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 142**
DLP and Geo Policy are examples of what type of Policy?

A. Standard Policies
B. Shared Policies
C. Inspection Policies
D. Unified Policies

**Answer:** B

**NEW QUESTION 143**
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 148**
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 150**
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 152**
What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes to complete.
B. Threat Extraction always delivers a file and takes less than a second to complete.
C. Threat Emulation never delivers a file that takes less than a second to complete.
D. Threat Extraction never delivers a file and takes more than 3 minutes to complete.

**Answer:** B

**NEW QUESTION 154**
On what port does the CPM process run?

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

**Answer:** D

**NEW QUESTION 159**
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 162**
Which statement is true regarding redundancy?

A. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob –f if command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Machines in a ClusterXL High Availability configuration must be synchronized.
D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

**Answer:** D

**NEW QUESTION 166**
To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:

A. fw ctl multik set_mode 1
B. fw ctl Dynamic_Priority_Queue on
C. fw ctl Dynamic_Priority_Queue enable
D. fw ctl multik set_mode 9

**Answer:** D

**NEW QUESTION 167**
Which of the following is NOT an alert option?

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

**Answer:** B

**NEW QUESTION 169**
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 173**
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 178**
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 182**
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 187**
What is the difference between SSL VPN and IPSec VPN?

A. IPSec VPN does not require installation of a resilient VPN client.
B. SSL VPN requires installation of a resident VPN client.
C. SSL VPN and IPSec VPN are the same.
D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser.

**Answer:** D

**NEW QUESTION 191**
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 193**
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 197**

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 202**
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 207**
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 211**
Fill in the blank: A _____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

A. Clientless remote access
B. Clientless direct access
C. Client-based remote access
D. Direct access

**Answer:** A

**NEW QUESTION 216**
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 ae 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 221**
What is correct statement about Security Gateway and Security Management Server failover in Check Point R80.X in terms of Check Point Redundancy driven solution?

A. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
B. Security Gateway failover as well as Security Management Server failover is a manual procedure.
C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
D. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

**Answer:** A

**NEW QUESTION 224**
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 tas
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 229**
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 231**
When gathering information about a gateway using CPINFO, what information is included or excluded when using the “-x” parameter?

A. Includes the registry
B. Gets information about the specified Virtual System
C. Does not resolve network addresses
D. Output excludes connection table

**Answer:** B

**NEW QUESTION 236**
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 238**
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 241**
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 246**
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 247**
What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

A. Source address, Destination address, Source port, Destination port, Protocol
B. Source MAC address, Destination MAC address, Source port, Destination port, Protocol
C. Source address, Destination address, Source port, Destination port
D. Source address, Destination address, Destination port, Protocol

**Answer:** A

**NEW QUESTION 249**
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 254**
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

A. Accept; redirect
B. Accept; drop
C. Redirect; drop
D. Drop; accept

**Answer:** D

**NEW QUESTION 258**
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

A. ThreatWiki
B. Whitelist Files
C. AppWiki
D. IPS Protections

**Answer:** B

**NEW QUESTION 263**
Which remote Access Solution is clientless?

A. Checkpoint Mobile
B. Endpoint Security Suite
C. SecuRemote
D. Mobile Access Portal

**Answer:** D

**NEW QUESTION 264**
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 268**
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 273**
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 276**
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

A. Symmetric routing
B. Failovers
C. Asymmetric routing
D. Anti-Spoofing

**Answer:** C

**NEW QUESTION 279**
What command verifies that the API server is responding?

A. api stat
B. api status
C. show api_status
D. app_get_status

**Answer:** B

**NEW QUESTION 280**
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 Kernal, 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 283**
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 286**
Check Pont Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____ .

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

**Answer:** D

**NEW QUESTION 290**
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 292**
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 296**
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 298**
What is the difference between an event and a log?

A. Events are generated at gateway according to Event Policy
B. A log entry becomes an event when it matches any rule defined in Event Policy
C. Events are collected with SmartWorkflow form Trouble Ticket systems
D. Log and Events are synonyms

**Answer:** B

**NEW QUESTION 299**
How many layers make up the TCP/IP model?

A. 2
B. 7
C. 6
D. 4

**Answer:** D

**NEW QUESTION 303**
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 307**
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 309**
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 310**
If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

A. Nothing - the proxy ARP is automatically handled in the R80 version
B. Add the proxy ARP configurations in a file called /etc/conf/local.arp
C. Add the proxy ARP configurations in a file called $FWDIR/conf/local.arp
D. Add the proxy ARP configurations in a file called $CPDIR/conf/local.arp

**Answer:** D

**NEW QUESTION 315**
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 319**
Where do you create and modify the Mobile Access policy in R80?

A. SmartConsole
B. SmartMonitor
C. SmartEndpoint
D. SmartDashboard

**Answer:** A

**NEW QUESTION 320**
Office mode means that:

A. SecurID client assigns a routable MAC addres
B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
C. Users authenticate with an Internet browser and use secure HTTPS connection.
D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
E. Allows a security gateway to assign a remote client an IP addres
F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

**Answer:** D

**NEW QUESTION 324**
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 328**
Which application should you use to install a contract file?

A. SmartView Monitor
B. WebUI
C. SmartUpdate
D. SmartProvisioning

**Answer:** C

**NEW QUESTION 332**
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 335**
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 338**
You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

A. sim erdos –e 1
B. sim erdos – m 1
C. sim erdos –v 1
D. sim erdos –x 1

**Answer:** A

**NEW QUESTION 343**
What are the blades of Threat Prevention?

A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
C. IPS, AntiVirus, AntiBot
D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

**Answer:** D

**NEW QUESTION 348**
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 349**
What is true about VRRP implementations?

A. VRRP membership is enabled in cpconfig
B. VRRP can be used together with ClusterXL, but with degraded performance
C. You cannot have a standalone deployment
D. You cannot have different VRIDs in the same physical network

**Answer:** C

**NEW QUESTION 352**
What has to be taken into consideration when configuring Management HA?

A. The Database revisions will not be synchronized between the management servers
B. SmartConsole must be closed prior to synchronized changes in the objects database
C. If you wanted to use Full Connectivity Upgrade, you must change the Implied Rules to allow FW1_cpredundant to pass before the Firewall Control Connections.
D. For Management Server synchronization, only External Virtual Switches are supporte
E. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.

**Answer:** A

**NEW QUESTION 355**
Which command is used to obtain the configuration lock in Gaia?

A. Lock database override
B. Unlock database override
C. Unlock database lock
D. Lock database user

**Answer:** A

**Explanation:**
Obtaining a Configuration Lock

**NEW QUESTION 357**
Which one of the following is true about Capsule Connect?

A. It is a full layer 3 VPN client
B. It offers full enterprise mobility management
C. It is supported only on iOS phones and Windows PCs
D. It does not support all VPN authentication methods

**Answer:** A

**NEW QUESTION 362**
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____ .

A. Firewall policy install
B. Threat Prevention policy install
C. Anti-bot policy install
D. Access Control policy install

**Answer:** C

**Explanation:**

https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents

**NEW QUESTION 364**
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode

**Answer:** C

**Explanation:**
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

**NEW QUESTION 369**
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 374**
What is the benefit of “tw 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 377**
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment

**Answer:** D

**NEW QUESTION 378**
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

A. Accounting
B. Suppression
C. Accounting/Suppression
D. Accounting/Extended

**Answer:** C

**NEW QUESTION 380**
Which firewall daemon is responsible for the FW CLI commands?

A. fwd
B. fwm
C. cpm
D. cpd

**Answer:** A

**NEW QUESTION 385**
.....

# 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