# Check-Point

## Exam Questions 156-315.80

Check Point Certified Security Expert - R80

**NEW QUESTION 1**
Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R80.10 SmartConsole application?

A. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
B. Firewall, IPS, Threat Emulation, Application Control.
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
D. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.

**Answer:** C

**NEW QUESTION 2**
Which of the SecureXL templates are enabled by default on Security Gateway?

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

**Answer:** D

**NEW QUESTION 3**
Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

A. enable DLP and select.exe and .bat file type
B. enable .exe & .bat protection in IPS Policy
C. create FW rule for particular protocol
D. tecli advanced attributes set prohibited_file_types exe.bat

**Answer:** A

**NEW QUESTION 4**
What is the default size of NAT table fwx_alloc?

A. 20000
B. 35000
C. 25000
D. 10000

**Answer:** C

**NEW QUESTION 5**
In a Client to Server scenario, which represents that the packet has already checked against the tables and the Rule Base?

A. Big I
B. Little o
C. Little i
D. Big O

**Answer:** D

**NEW QUESTION 6**
Which of the following is a task of the CPD process?

A. Invoke and monitor critical processes and attempts to restart them if they fail
B. Transfers messages between Firewall processes
C. Log forwarding
D. Responsible for processing most traffic on a security gateway

**Answer:** A

**Explanation:**
https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12496.htm

**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**
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 9**
What is the valid range for VRID value in VRRP configuration?

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

**Answer:** B

**Explanation:**
Virtual Router ID - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255. \

**NEW QUESTION 10**
Which command can you use to verify the number of active concurrent connections?

A. fw conn all
B. fw ctl pstat
C. show all connections
D. show connections

**Answer:** B

**NEW QUESTION 10**
What kind of information would you expect to see using the sim affinity command?

A. The VMACs used in a Security Gateway cluster
B. The involved firewall kernel modules in inbound and outbound packet chain
C. Overview over SecureXL templated connections
D. Network interfaces and core distribution used for CoreXL

**Answer:** D

**NEW QUESTION 14**
Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

A. assign privileges to users.
B. edit the home directory of the user.
C. add users to your Gaia system.
D. assign user rights to their home directory in the Security Management Server.

**Answer:** D

**NEW QUESTION 16**
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 17**
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 foun
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 22**
What is the name of the secure application for Mail/Calendar for mobile devices?

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

**Answer:** A

**NEW QUESTION 25**
You can access the ThreatCloud Repository from:

A. R80.10 SmartConsole and Application Wiki
B. Threat Prevention and Threat Tools
C. Threat Wiki and Check Point Website
D. R80.10 SmartConsole and Threat Prevention

**Answer:** D

**NEW QUESTION 27**
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 28**
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 31**
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 34**
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 37**
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 41**
Which statement is correct about the Sticky Decision Function?

A. It is not supported with either the Performance pack of a hardware based accelerator card
B. Does not support SPI's when configured for Load Sharing
C. It is automatically disabled if the Mobile Access Software Blade is enabled on the cluster
D. It is not required L2TP traffic

**Answer:** A

**NEW QUESTION 42**
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 43**
What is the responsibility of SOLR process on R80.10 management server?

A. Validating all data before it's written into the database
B. It generates indexes of data written to the database
C. Communication between SmartConsole applications and the Security Management Server
D. Writing all information into the database

**Answer:** B

**NEW QUESTION 46**
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 47**
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 52**
What is the command to show SecureXL status?

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

**Answer:** D

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

**NEW QUESTION 56**
What can we infer about the recent changes made to the Rule Base?

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

**Answer:** D

**NEW QUESTION 59**
You are investigating issues with to gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

A. TCP port 443
B. TCP port 257
C. TCP port 256
D. UDP port 8116

**Answer:** C

**NEW QUESTION 60**
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 65**
Which process handles connection from SmartConsole R80?

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

**Answer:** C

**NEW QUESTION 68**
You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the tight protections in place. Check Point has been selected for the security vendor.
Which Check Point product protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

A. IPS AND Application Control
B. IPS, anti-virus and anti-bot
C. IPS, anti-virus and e-mail security
D. SandBlast

**Answer:** D

**NEW QUESTION 72**
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 75**
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

**Answer:** B

**NEW QUESTION 78**
John is using Management HA. Which Smartcenter should be connected to for making changes?

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

**Answer:** B

**NEW QUESTION 80**
Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?

A. Severity
B. Automatic reactions
C. Policy
D. Threshold

**Answer:** C

**NEW QUESTION 84**
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 86**
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 check box 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 89**
What is the least amount of CPU cores required to enable CoreXL?

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

**Answer:** B

**NEW QUESTION 91**
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 94**
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 99**

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 102**
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 103**
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

**Answer:** D

**NEW QUESTION 106**
What component of R80 Management is used for indexing?

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

**Answer:** D

**NEW QUESTION 111**
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.

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

**Answer:** D

**NEW QUESTION 113**
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 114**
GAiA Software update packages can be imported and installed offline in situation where:

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

**Answer:** B

**NEW QUESTION 115**
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 119**
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 123**
SmartConsole R80 requires the following ports to be open for SmartEvent R80 management:

A. 19090,22
B. 19190,22
C. 18190,80
D. 19009,443

**Answer:** D

**NEW QUESTION 127**
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 130**
What is the limitation of employing Sticky Decision Function?

A. With SDF enabled, the involved VPN Gateways only supports IKEv1
B. Acceleration technologies, such as SecureXL and CoreXL are disabled when activating SDF
C. With SDF enabled, only ClusterXL in legacy mode is supported
D. With SDF enabled, you can only have three Sync interfaces at most

**Answer:** B

**NEW QUESTION 134**
Which encryption algorithm is the least secured?

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

**Answer:** C

**NEW QUESTION 137**
Which command would disable a Cluster Member permanently?

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

**Answer:** C

**NEW QUESTION 142**
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 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 145**
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 147**
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

A. Toni? AND 10.0.4.210 NOT 10.0.4.76
B. To** AND 10.0.4.210 NOT 10.0.4.76
C. Ton* AND 10.0.4.210 NOT 10.0.4.75
D. "Toni" AND 10.0.4.210 NOT 10.0.4.76

**Answer:** B

**NEW QUESTION 151**
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 156**
Which path below is available only when CoreXL is enabled?

A. Slow path
B. Firewall path
C. Medium path
D. Accelerated path

**Answer:** C

**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 161**
You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

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

**Answer:** A

**NEW QUESTION 162**
CoreXL is supported when one of the following features is enabled:

A. Route-based VPN
B. IPS
C. IPv6
D. Overlapping NAT

**Answer:** B

**Explanation:**
CoreXL does not support Check Point Suite with these features: References:

**NEW QUESTION 163**
Which Check Point software blade provides Application Security and identity control?

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

**Answer:** D

**NEW QUESTION 166**
Which of the following process pulls application monitoring status?

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

**Answer:** D

**NEW QUESTION 170**
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 174**
What is the default shell for the command line interface?

A. Expert
B. Clish
C. Admin
D. Normal

**Answer:** B

**Explanation:**
The default shell of the CLI is called clish

**NEW QUESTION 175**
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 179**
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 181**
What is considered Hybrid Emulation Mode?

A. Manual configuration of file types on emulation location.
B. Load sharing of emulation between an on premise appliance and the cloud.
C. Load sharing between OS behavior and CPU Level emulation.
D. High availability between the local SandBlast appliance and the cloud.

**Answer:** B

**NEW QUESTION 182**
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 186**
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 190**
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 194**
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 195**
How long may verification of one file take for Sandblast Threat Emulation?

A. up to 1 minutes
B. within seconds cleaned file will be provided

C. up to 5 minutes
D. up to 3 minutes

**Answer:** B

**NEW QUESTION 196**
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 201**
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 202**
Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.

A. Better understand the behavior of the Access Control Policy
B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base
C. Automatically rearrange Access Control Policy based on Hit Count Analysis
D. Analyze a Rule Base - You can delete rules that have no matching connections

**Answer:** C

**NEW QUESTION 203**
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 205**
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 210**
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 211**
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 214**
One of major features in R80 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

A. A lock icon shows that a rule or an object is locked and will be available.
B. AdminA and AdminB are editing the same rule at the same time.
C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

**Answer:** C

**NEW QUESTION 218**
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 223**
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 227**
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 232**
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 233**
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 237**
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 242**
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 244**
Which one of the following is true about Threat Extraction?

A. Always delivers a file to user
B. Works on all MS Office, Executables, and PDF files
C. Can take up to 3 minutes to complete
D. Delivers file only if no threats found

**Answer:** A

**NEW QUESTION 248**
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 253**
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

A. All UDP packets
B. All IPv6 Traffic
C. All packets that match a rule whose source or destination is the Outside Corporate Network
D. CIFS packets

**Answer:** D

**NEW QUESTION 254**
Joey want to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

A. https://<Device_IP_Adress>
B. http://<Device IP_Address>:443
C. https://<Device_IP_Address>:10000
D. https://<Device_IP_Address>:4434

**Answer:** A

**NEW QUESTION 255**
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 260**
Fill in the blank: An identity server uses a _____ for user authentication.

A. Shared secret
B. Certificate
C. One-time password
D. Token

**Answer:** A

**NEW QUESTION 263**
How many layers make up the TCP/IP model?

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

**Answer:** D

**NEW QUESTION 267**
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 271**
What API command below creates a new host with the name “New Host” and IP address of “192.168.0.10”?

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

**Answer:** D

**NEW QUESTION 276**
What is the purpose of a SmartEvent Correlation Unit?

A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
B. The SmartEvent Correlation Unit’s task it to assign severity levels to the identified events.
C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.

**Answer:** C

**NEW QUESTION 281**
Where do you create and modify the Mobile Access policy in R80?

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

**Answer:** A

**NEW QUESTION 284**
You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.
What must you do to get SIC to work?

A. Remove Geo-Protection, as the IP-to-country database is updated externally, and you have no control of this.
B. Create a rule at the top in the Sydney firewall to allow control traffic from your network
C. Nothing - Check Point control connections function regardless of Geo-Protection policy
D. Create a rule at the top in your Check Point firewall to bypass the Geo-Protection

**Answer:** C

**NEW QUESTION 289**
Which command would you use to set the network interfaces’ affinity in Manual mode?

A. sim affinity -m
B. sim affinity -l
C. sim affinity -a
D. sim affinity -s

**Answer:** D

**NEW QUESTION 293**
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 296**
Joey wants to upgrade from R75.40 to R80 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this.
What is one of the requirements for his success?

A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine
B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
C. Size of the $FWDIR/log folder of the target machine must be at least 30% of the size of the$FWDIR/log directory on the source machine
D. Size of the /var/log folder of the target machine must be at least 25GB or more

**Answer:** B

**NEW QUESTION 298**
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 302**
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 307**
Check Point APIs allow system engineers and developers to make changes to their organization’s security policy with CLI tools and Web Services for all the following except:

A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution

**Answer:** A

**Explanation:**
Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
• Use an automated script to perform common tasks
• Integrate Check Point products with 3rd party solutions
• Create products that use and enhance the Check Point solution References:

**NEW QUESTION 312**
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 317**
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 320**
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported

**Answer:** A

**NEW QUESTION 322**
What are types of Check Point APIs available currently as part of R80.10 code?

A. Security Gateway API Management API, Threat Prevention API and Identity Awareness Web Services API
B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

**Answer:** B

**NEW QUESTION 325**
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 329**
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 330**
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 335**
What is the purpose of extended master key extension/session hash?

A. UDP VOIP protocol extension
B. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-servercommunication
C. Special TCP handshaking extension
D. Supplement DLP data watermark

**Answer:** B

**NEW QUESTION 340**
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 344**
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 347**
How can SmartView application accessed?

A. http://<Security Management IP Address>/smartview
B. http://<Security Management IP Address>:4434/smartview/
C. https://<Security Management IP Address>/smartview/
D. https://<Security Management host name>:4434/smartview/

**Answer:** C

**NEW QUESTION 349**
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 350**
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 351**
You have existing dbedit scripts from R77. Can you use them with R80.10?

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

**Answer:** D

**NEW QUESTION 354**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## 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