

## 156-315.80 Dumps

### Check Point Certified Security Expert - R80

<https://www.certleader.com/156-315.80-dumps.html>



**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**

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 3**

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

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

**Answer: D**

**NEW QUESTION 4**

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 5**

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path
- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

**Answer: D**

**NEW QUESTION 6**

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 7**

In R80 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

**Answer: D**

**Explanation:**

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware

and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

**NEW QUESTION 8**

The essential means by which state synchronization works to provide failover in the event an active member goes down, \_\_\_\_\_ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

- A. ccp
- B. cphaconf
- C. cphad
- D. cphastart

**Answer: A**

**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. \$FWDIR/smartevent/conf
- B. \$RTDIR/smartevent/conf
- C. \$RTDIR/smartview/conf
- D. \$FWDIR/smartview/conf

**Answer: C**

**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 13**

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 18**

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 19**

What is the correct order of the default "fw monitor" inspection points?

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

**Answer:** C

**NEW QUESTION 22**

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

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

**Answer:** B

**NEW QUESTION 23**

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 26**

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 27**

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 30**

Which process handles connection from SmartConsole R80?

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

**Answer:** C

**NEW QUESTION 33**

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 35**

What is the purpose of Priority Delta in VRRP?

- A. When a box up, Effective Priority = Priority + Priority Delta
- B. When an Interface is up, Effective Priority = Priority + Priority Delta
- C. When an Interface fail, Effective Priority = Priority – Priority Delta

D. When a box fail, Effective Priority = Priority – Priority Delta

**Answer:** C

**Explanation:**

Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will begin to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP. References:

**NEW QUESTION 37**

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 40**

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 41**

Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

- A. cpexport
- B. sysinfo
- C. cpsizeme
- D. cpinfo

**Answer:** C

**NEW QUESTION 43**

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 45**

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CApp

**Answer:** B

**NEW QUESTION 47**

What will SmartEvent automatically define as events?

- A. Firewall
- B. VPN
- C. IPS
- D. HTTPS

**Answer:** C

**NEW QUESTION 49**

Fill in the blank: Authentication rules are defined for \_\_\_\_\_.

- A. User groups
- B. Users using UserCheck

- C. Individual users
- D. All users in the database

**Answer:** A

**NEW QUESTION 52**

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 56**

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 60**

To optimize Rule Base efficiency, the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

**Answer:** C

**NEW QUESTION 63**

On R80.10 the IPS Blade is managed by:

- A. Threat Protection policy
- B. Anti-Bot Blade
- C. Threat Prevention policy
- D. Layers on Firewall policy

**Answer:** C

**NEW QUESTION 64**

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 69**

Fill in the blank: The R80 feature \_\_\_\_\_ permits blocking specific IP addresses for a specified time period.

- A. Block Port Overflow
- B. Local Interface Spoofing
- C. Suspicious Activity Monitoring
- D. Adaptive Threat Prevention

**Answer:** C

**Explanation:**

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.

References:

**NEW QUESTION 72**

Why would an administrator see the message below?

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

**Answer: B**

**NEW QUESTION 75**

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 76**

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 78**

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 83**

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 87**

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 92**

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 97**

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 101**

Which of the following process pulls application monitoring status?

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

**Answer: D**

**NEW QUESTION 106**

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 108**

View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)

- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

**Answer:** B

**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 110**

What SmartEvent component creates events?

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

**Answer:** B

**NEW QUESTION 114**

Advanced Security Checkups can be easily conducted within:

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

**Answer:** A

**NEW QUESTION 117**

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 121**

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 125**

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 126**

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 129**

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 130**

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 133**

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

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

**Answer:** C

**Explanation:**

One for Security Management Server and the other one for the Security Gateway.

**NEW QUESTION 136**

To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

- A. Accept Template
- B. Deny Template
- C. Drop Template
- D. NAT Template

**Answer:** B

**NEW QUESTION 138**

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

**Answer:** A

**NEW QUESTION 139**

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 142**

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 147**

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 151**

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

- A. All Connections (Clear or Encrypted)
- B. Accept all encrypted traffic
- C. Specific VPN Communities
- D. All Site-to-Site VPN Communities

**Answer: B**

**NEW QUESTION 153**

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

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

**Answer: C**

**NEW QUESTION 154**

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 158**

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 159**

How many layers make up the TCP/IP model?

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

**Answer: D**

**NEW QUESTION 163**

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 166**

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 171**

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

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

**Answer:** B

**NEW QUESTION 174**

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 178**

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

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

**Answer:** C

**NEW QUESTION 180**

What is the order of NAT priorities?

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

**Answer:** A

**NEW QUESTION 183**

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

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

**Answer:** A

**NEW QUESTION 187**

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 191**

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 193**

Using ClusterXL, what statement is true about the Sticky Decision Function?

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL

**Answer: A**

**NEW QUESTION 198**

Which application should you use to install a contract file?

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

**Answer: C**

**NEW QUESTION 199**

Where you can see and search records of action done by R80 SmartConsole administrators?

- A. In SmartView Tracker, open active log
- B. In the Logs & Monitor view, select "Open Audit Log View"
- C. In SmartAuditLog View
- D. In Smartlog, all logs

**Answer: B**

**NEW QUESTION 201**

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 205**

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 208**

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 209**

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 214**

How many images are included with Check Point TE appliance in Recommended Mode?

- A. 2(OS) images
- B. images are chosen by administrator during installation
- C. as many as licensed for
- D. the most new image

**Answer: A**

**NEW QUESTION 219**

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-server communication
- C. Special TCP handshaking extension
- D. Supplement DLP data watermark

**Answer: B**

**NEW QUESTION 221**

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 225**

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 227**

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 231**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 156-315.80 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/156-315.80-dumps.html>