# 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**
The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

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

**Answer:** A

**NEW QUESTION 3**
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with _______ will not apply.

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

**Answer:** B

**NEW QUESTION 4**
What is UserCheck?

A. Messaging tool used to verify a user's credentials.
B. Communication tool used to inform a user about a website or application they are trying to access.
C. Administrator tool used to monitor users on their network.
D. Communication tool used to notify an administrator when a new user is created.

**Answer:** B

**NEW QUESTION 5**
Which of the following is NOT a component of Check Point Capsule?

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

**Answer:** C

**NEW QUESTION 6**
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 7**
In a Client to Server scenario, which represents that the packet has already checked against the tables and the Rule Base?

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

**Answer:** D

**NEW QUESTION 8**
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 9**
John detected high load on sync interface. Which is most recommended solution?

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

**Answer:** A

**NEW QUESTION 10**
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 10**
Which of the following describes how Threat Extraction functions?

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

**Answer:** B

**NEW QUESTION 11**
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

**Answer:** D

**NEW QUESTION 16**
What statement best describes the Proxy ARP feature for Manual NAT in R80.10?

A. Automatic proxy ARP configuration can be enabled
B. Translate Destination on Client Side should be configured
C. fw ctl proxy should be configured
D. local.arp file must always be configured

**Answer:** D

**NEW QUESTION 17**
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 22**
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 25**
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 26**
Which of the following is NOT a VPN routing option available in a star community?

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

**Answer:** AD

**NEW QUESTION 30**
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 33**
SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?

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

**Answer:** B

**NEW QUESTION 38**
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 39**
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 40**
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 43**
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 45**
What are the two high availability modes?

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

**Answer:** D

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

**NEW QUESTION 46**
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 47**
What is the most ideal Synchronization Status for Security Management Server High Availability deployment?

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

**Answer:** B

**NEW QUESTION 49**
Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

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

**Answer:** B

**NEW QUESTION 51**
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 56**
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 61**
To add a file to the Threat Prevention Whitelist, what two items are needed?

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

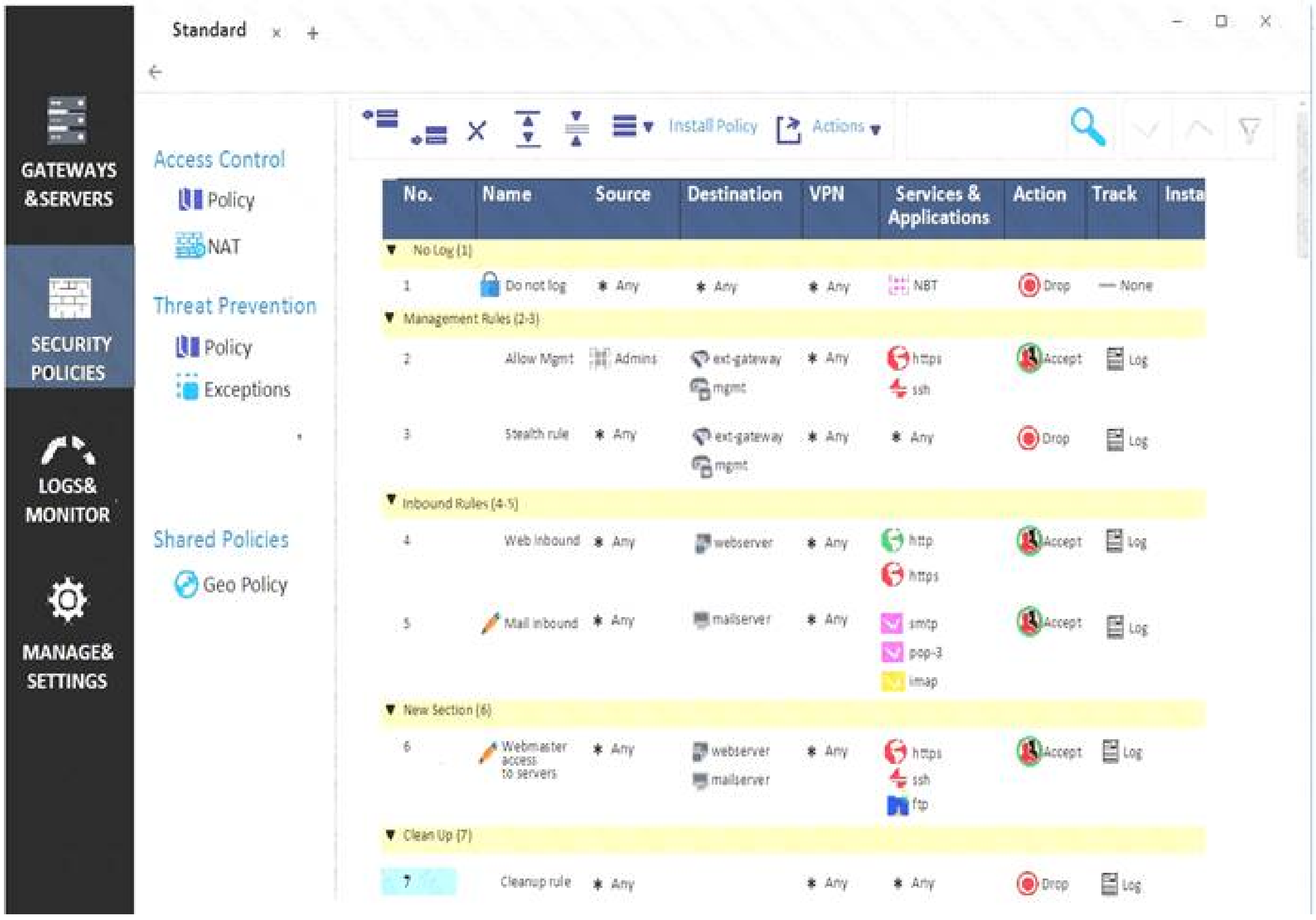
**Answer:** B

**NEW QUESTION 62**
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 64**
What can we infer about the recent changes made to the Rule Base?



| No. | Name | Source | Destination | VPN | Services & Applications | Action | Track | Insta |
|---|---|---|---|---|---|---|---|---|
| ▼ No Log (1) | | | | | | | | |
| 1 | Do not log | * Any | * Any | * Any | NBT | Drop | — None | |
| ▼ Management Rules (2-3) | | | | | | | | |
| 2 | Allow Mgmt | Admins | ext-gateway<br>mgmt | * Any | https<br>ssh | Accept | Log | |
| 3 | Stealth rule | * Any | ext-gateway<br>mgmt | * Any | * Any | Drop | Log | |
| ▼ Inbound Rules (4-5) | | | | | | | | |
| 4 | Web Inbound | * Any | webserver | * Any | http<br>https | Accept | Log | |
| 5 | Mail inbound | * Any | mailserver | * Any | smtp<br>pop-3<br>imap | Accept | Log | |
| ▼ New Section (6) | | | | | | | | |
| 6 | Webmaster access to servers | * Any | webserver<br>mailserver | * Any | https<br>ssh<br>ftp | Accept | Log | |
| ▼ Clean Up (7) | | | | | | | | |
| 7 | Cleanup rule | * Any | | * Any | * Any | Drop | Log | |

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 68**
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 72**
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 76**
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 79**
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 81**
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 beging 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 82**
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 83**
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 86**
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 90**
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 92**
What is the least amount of CPU cores required to enable CoreXL?

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

**Answer:** B

**NEW QUESTION 93**
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 98**
Which Check Point feature enables application scanning and the detection?

A. Application Dictionary
B. AppWiki
C. Application Library
D. CPApp

**Answer:** B

**NEW QUESTION 101**
Which is NOT an example of a Check Point API?

A. Gateway API
B. Management API
C. OPSEC SDK
D. Threat Prevention API

**Answer:** A

**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**
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 113**
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 118**
When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

A. Network, and defining your Class A space
B. Topology, and you are defining the Internal network
C. Internal addresses you are defining the gateways
D. Internal network(s) you are defining your networks

**Answer:** B

**NEW QUESTION 123**
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 128**
When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:

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

**Answer:** D

**NEW QUESTION 129**
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R80.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned O
B. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OF
D. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
E. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
F. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

**Answer:** A

**NEW QUESTION 132**
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 137**
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 141**
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 143**
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 147**
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 151**
Which of the following process pulls application monitoring status?

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

**Answer:** D

**NEW QUESTION 153**
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 158**
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
C. Mail, Block Source, Block Destination, External Script, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

**Answer:** A

**NEW QUESTION 163**
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 167**
Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or via CLI.
Which command should he use in CLI? (Choose the correct answer.)

A. remove database lock
B. The database feature has one command lock database override.
C. override database lock
D. The database feature has two commands lock database override and unlock databas
E. Both will work.

**Answer:** D

**NEW QUESTION 172**
What SmartEvent component creates events?

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

**Answer:** B

**NEW QUESTION 176**
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 177**
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 179**
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 180**
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 185**
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 186**
Which is NOT a SmartEvent component?

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

**Answer:** C

**NEW QUESTION 190**
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 195**
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 200**
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 205**
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 210**
Which two of these Check Point Protocols are used by SmartEvent Processes?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

**Answer:** D

**NEW QUESTION 211**
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 213**
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 215**
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 220**
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 222**
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 225**
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 227**
When requiring certificates for mobile devices, make sure the authentication method is set to one of the following, Username and Password, RADIUS or _____.

A. SecureID
B. SecurID
C. Complexity
D. TacAcs

**Answer:** B

**NEW QUESTION 231**
What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
D. Go to Application&url filtering blade > Https Inspection > Policy

**Answer:** A

**NEW QUESTION 234**
When simulating a problem on ClusterXL cluster with cphaprob –d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command

allows you remove the problematic state?

A. cphaprob –d STOP unregister
B. cphaprob STOP unregister
C. cphaprob unregister STOP
D. cphaprob –d unregister STOP

**Answer:** A

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

**NEW QUESTION 237**
Which remote Access Solution is clientless?

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

**Answer:** D

**NEW QUESTION 242**
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 246**
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 250**
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 254**
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 256**
Which of these is an implicit MEP option?

A. Primary-backup
B. Source address based
C. Round robin
D. Load Sharing

**Answer:** A

**NEW QUESTION 261**
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 264**
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 266**
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 269**
Which CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat
B. ips pstats reset
C. ips pmstats refresh
D. ips pmstats reset

**Answer:** D

**NEW QUESTION 270**
In the Firewall chain mode FFF refers to:

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

**Answer:** C

**NEW QUESTION 273**
What Factor preclude Secure XL Templating?

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

**Answer:** A

**NEW QUESTION 277**
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 280**

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 284**
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 289**
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 293**
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 296**
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 299**
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 300**
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _______ .

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

**Answer:** A

**NEW QUESTION 305**
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 309**
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 313**
......