IT-Exams.com®
Easiest way to pass any IT exams

-The original certification question!

https://www.it-exams.com

Exam Number: 156-315.80

Exam Name: Check Point Certified Security Expert - R80

Version: Demo

Q1
Identify the API that is not supported by Check Point currently.

A. R80 Management API-
B. Identity Awareness Web Services API
C. Open REST API
D. OPSEC SDK

Answer: C

Q2
SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data. Which component is NOT part of the SandBlast Mobile solution?

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

Answer: C

Reference:
https://community.checkpoint.com/docs/DOC-3072-sandblast-mobile-architecture-overview

Q3
What are the different command sources that allow you to communicate with the API server?

A. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
B. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
C. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
D. API_cli Tool, Gaia CLI, Web Services

Answer: B

Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction%20

Q4
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

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_AntiBotAntiVirus_AdminGuide/index.html

Q5
Which TCP-port does CPM process listen to?

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

Answer: D

Reference:
https://www.checkpoint.com/downloads/products/r80.10-security-management-architecture-overview.pdf

Q6
Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using the "mgmt_cli" command
B. Typing API commands from a dialog box inside the SmartConsole GUI application

C. Typing API commands using Gaia's secure shell(clish)19+
D. Sending API commands over an http connection using web-services

Answer: D

Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction%20

Q7
Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to manager?

A. fw accel stat
B. fwaccel stat
C. fw acces stats
D. fwaccel stats

Answer: B

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk41397

Q8
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

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk67820

Q9
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

Q10
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

Q11
Fill in the blank: The tool _____ generates a R80 Security Gateway configuration report.

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

Answer: C

Q12
Which of these statements describes the Check Point ThreatCloud?

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

D. A worldwide collaborative security network

Answer: D

Q13
Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

A. 15 sec
B. 60 sec
C. 5 sec
D. 30 sec

Answer: B

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

Q14
Which command will allow you to see the interface status?

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

Answer: C

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

Q15
Which command can you use to enable or disable multi-queue per interface?

A. cpmq set
B. Cpmqueue set
C. Cpmq config

D. Set cpmq enable

Answer: A

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/93689.htm

Q16
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

Reference: http://dl3.checkpoint.com/paid/21/CP_R76_SmartEventIntro_AdminGuide.pdf?HashKey=1538417023_7cb74dfe0e109c21f130f556d419faaf&xtn=.pdf

Q17
There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

A. Using Web Services
B. Using Mgmt_cli tool
C. Using CLISH
D. Using SmartConsole GUI console
E. Events are collected with SmartWorkflow from Trouble Ticket systems

Answer: E

Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction%20

Q18
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:
Check Point QoS (Quality of Service)

Route-based VPN

IPv6 on IPSO

Overlapping NAT

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

Q19
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

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105261

Q20
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

Q21
Which command is used to set the CCP protocol to Multicast?

A. cphaprob set_ccp multicast
B. cphaconf set_ccp multicast
C. cphaconf set_ccp no_broadcast
D. cphaprob set_ccp no_broadcast

Answer: B

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk20576

Q22
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

Reference: http://trlj.blogspot.com/2015/10/check-point-acceleration.html

Q23

Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

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

Answer: D

Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/120712

Q24
During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

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

Answer: D

Q25
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.
Reference:
http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?HashKey=1479584563_6f823c8ea1514609148aa4fec5425db2&xtn=.pdf

Q26
Connections to the Check Point R80 Web API use what protocol?

A. HTTPS
B. RPC
C. VPN
D. SIC

Answer: A

Q27
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

Reference: http://dl3.checkpoint.com/paid/c7/c76b823d81bab77e1e40ac086fa81411/CP_R77_versions_CLI_ReferenceGuide.pdf?HashKey=1538418170_96def40f213f24a8b273cc77b408dd3f&xtn=.pdf

Q28
What is true about the IPS-Blade?

A. In R80, IPS is managed by the Threat Prevention Policy
B. In R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict

C. In R80, IPS Exceptions cannot be attached to "all rules"
D. In R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

Q29
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

A. Detects and blocks malware by correlating multiple detection engines before users are affected.
B. Configure rules to limit the available network bandwidth for specified users or groups.
C. Use UserCheck to help users understand that certain websites are against the company's security policy.
D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm

Q30
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".
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30974

Q31
What Factor preclude Secure XL Templating?

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

Answer: A

Q32
In order to get info about assignment (FW, SND) of all CPUs in your SGW, what is the most accurate CLI command?

A. fw ctl sdstat
B. fw ctl affinity -l -a -r -v
C. fw ctl multik stat
D. cpinfo

Answer: B

Q33
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

Q34
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

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

Q35
What is not a component of Check Point SandBlast?

A. Threat Emulation
B. Threat Simulator
C. Threat Extraction
D. Threat Cloud

Answer: B