Check Point Certified Security Expert (CCSE)

# Exam 156-315.81 Check Point Security Expert R81 (CCSE)

Demo Questions

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT CERTIFIED
SECURITY EXPERT
CCSE

# 156-315.81 Check Point Certified Security Expert (CCSE) R81

Q.1
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

Q.2
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

Q.3
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.
A. This statement is true because SecureXL does improve all traffic.
B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
C. This statement is true because SecureXL does improve this traffic.
D. This statement is false because encrypted traffic cannot be inspected.

Answer: C
Explanation:
SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

Q.4
With SecureXL enabled, accelerated packets will pass through the following:
A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
B. Network Interface Card, Check Point Firewall Kernel, and the Acceleration Device
C. Network Interface Card and the Acceleration Device
D. Network Interface Card, OSI Network Layer, and the Acceleration Device

Answer: C

Q.5
Which TCP port does the CPM process listen on?
A. 18191
B. 18190
C. 8983
D. 19009

Answer: D

Q.6
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?
A. None, Security Management Server would be installed by itself.
B. SmartConsole
C. SecureClient
D. Security Gateway
E. SmartEvent

Answer: D

Q.7
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

Q.8
After the initial installation on Check Point appliance, you notice that the Management-interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.
A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24
set static-route default nexthop gateway address 192.168.80.1 onsave config
B. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24
add static-route default nexthop gateway address 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
D. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config

Answer: A

Q.9
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?
A. Slow Path
B. Medium Path
C. Fast Path
D. Accelerated Path

Answer: A

Q.10
Which packet info is masked with Session Rate Acceleration?
A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used

Answer: C

Q.11
Which command shows the current connections distributed by CoreXL FW instances?
A. fw ctl multik stat
B. fw ctl affinity -l
C. fw ctl instances -v
D. fw ctl iflist

Answer: A

Q.12
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

Q.13
Which of the following process pulls application monitoring status?
A. fwd
B. fwm
C. cpwd
D. cpd

Answer: D

Q.14
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

Q.15
The Security Gateway is installed on GAIA R81. The default port for the Web User Interface is _____ .
A. TCP 18211
B. TCP 257
C. TCP 4433
D. TCP 443

Answer: D

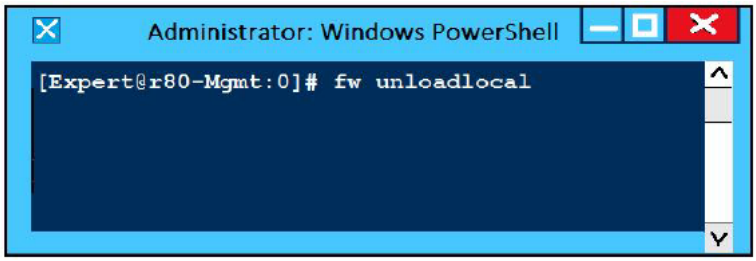
Q.16
In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?
A. Limit
B. Resource
C. Custom Application / Site
D. Network Object

Answer: B

Q.17
Which view is NOT a valid CPVIEW view?
A. IDA
B. RAD
C. PDP
D. VPN

Answer: C

Q.18
What will be the effect of running the following command on the Security Management Server?




A. Remove the installed Security Policy.
B. Remove the local ACL lists.
C. Reset SIC on all gateways.
D. No effect.

Answer: A

Q.19
Which SmartConsole tab is used to monitor network and security performance?
A. Manage Setting
B. Security Policies
C. Gateway and Servers
D. Logs and Monitor

Answer: D

Q.20
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 dat a.
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

Q.21
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

Q.22
Which command shows detailed information about VPN tunnels?
A. cat $FWDIR/conf/vpn.conf
B. vpn tu tlist
C. vpn tu
D. cpview

Answer: B

Q.23
Where do you create and modify the Mobile Access policy in R81?
A. SmartConsole
B. SmartMonitor
C. SmartEndpoint
D. SmartDashboard

Answer: A

Q.24
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

Q.25
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

Q.26
Which tool is used to enable ClusterXL?
A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Answer: B

Q.27
How many policy layers do Access Control policy support?
A. 2
B. 4
C. 1
D. 3

Answer: A
Explanation: Two policy layers: -Network Policy Layer -Application Control Policy Layer

Q.28
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

Q.29
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

Q.30
Which features are only supported with R80.10 Gateways but not R77.x?
A. Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
D. Time object to a rule to make the rule active only during specified times.

Answer: C

Q.31
Connections to the Check Point R81 Web API use what protocol?
A. HTTPS
B. RPC
C. VPN
D. SIC

Answer: A

Q.32
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