CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

NEW QUESTION 1
- (Exam Topic 1)
Which of the SecureXL templates are enabled by default on Security Gateway?

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

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
Which view is NOT a valid CPVIEW view?

A. IDA
B. RAD
C. PDP
D. VPN

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (Exam Topic 1)
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 5
- (Exam Topic 1)
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 6
- (Exam Topic 1)
Which TCP-port does CPM process listen to?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
Fill in the blank: The command _____ provides the most complete restoration of a R81 configuration.

A. upgrade_import
B. cpconfig
C. fwm dbimport -p <export file>
D. cpinfo –recover

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
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 10
- (Exam Topic 1)
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

NEW QUESTION 10
- (Exam Topic 1)
What happen when IPS profile is set in Detect Only Mode for troubleshooting?

A. It will generate Geo-Protection traffic
B. Automatically uploads debugging logs to Check Point Support Center
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control

Answer: C

Explanation:
It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic.
During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION 12
- (Exam Topic 1)
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 14
- (Exam Topic 1)
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 15
- (Exam Topic 1)
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 18
- (Exam Topic 1)
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 20
- (Exam Topic 1)
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

NEW QUESTION 21
- (Exam Topic 1)
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 23
- (Exam Topic 1)
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 27
- (Exam Topic 1)
Connections to the Check Point R81 Web API use what protocol?

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

Answer: A

NEW QUESTION 31
- (Exam Topic 1)
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 35
- (Exam Topic 1)
What is the difference between an event and a log?

A. Events are generated at gateway according to Event Policy
B. A log entry becomes an event when it matches any rule defined in Event Policy
C. Events are collected with SmartWorkflow form Trouble Ticket systems
D. Log and Events are synonyms

Answer: B

NEW QUESTION 38
- (Exam Topic 1)
In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?

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

Answer: A

NEW QUESTION 40
- (Exam Topic 1)
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

A. 50%
B. 75%
C. 80%
D. 15%

Answer: D

NEW QUESTION 44
- (Exam Topic 1)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 45
- (Exam Topic 1)
To fully enable Dynamic Dispatcher on a Security Gateway:

A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
B. Using cpconfig, update the Dynamic Dispatcher value to “full” under the CoreXL menu.
C. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
D. run fw multik set_mode 1 in Expert mode and then reboot.

Answer: A

NEW QUESTION 49
- (Exam Topic 1)
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: B

NEW QUESTION 52
- (Exam Topic 1)
You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup
B. import backup

C. cp_merge
D. migrate import

Answer: D

NEW QUESTION 54
- (Exam Topic 1)
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 59
- (Exam Topic 2)
What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes to complete.
B. Threat Extraction always delivers a file and takes less than a second to complete.
C. Threat Emulation never delivers a file that takes less than a second to complete.
D. Threat Extraction never delivers a file and takes more than 3 minutes to complete.

Answer: B

NEW QUESTION 60
- (Exam Topic 2)
Which GUI client is supported in R81?

A. SmartProvisioning
B. SmartView Tracker
C. SmartView Monitor
D. SmartLog

Answer: C

NEW QUESTION 64
- (Exam Topic 2)
Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

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

Answer: D

Explanation:
Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that requite direct GUI access, such as SmartEvent,
It provides the following:
– GUI Client communication
– Database manipulation
– Policy Compilation
– Management HA sync

NEW QUESTION 65
- (Exam Topic 2)
Under which file is the proxy arp configuration stored?

A. $FWDIR/state/proxy_arp.conf on the management server
B. $FWDIR/conf/local.arp on the management server
C. $FWDIR/state/_tmp/proxy.arp on the security gateway
D. $FWDIR/conf/local.arp on the gateway

Answer: D

NEW QUESTION 67
- (Exam Topic 2)
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
- (Exam Topic 2)
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 73
- (Exam Topic 2)
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 76
- (Exam Topic 2)
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 78
- (Exam Topic 2)
What command can you use to have cpinfo display all installed hotfixes?

A. cpinfo -hf
B. cpinfo –y all
C. cpinfo –get hf
D. cpinfo installed_jumbo

Answer: B

NEW QUESTION 80
- (Exam Topic 2)
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 83
- (Exam Topic 2)
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 88
- (Exam Topic 2)
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 93
- (Exam Topic 2)
Which one of the following is true about Capsule Connect?

A. It is a full layer 3 VPN client
B. It offers full enterprise mobility management
C. It is supported only on iOS phones and Windows PCs
D. It does not support all VPN authentication methods

Answer: A

NEW QUESTION 94
- (Exam Topic 2)
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 95
- (Exam Topic 2)
When installing a dedicated R81 SmartEvent server. What is the recommended size of the root partition?

A. Any size
B. Less than 20GB
C. More than 10GB and less than 20GB
D. At least 20GB

Answer: D

NEW QUESTION 100
- (Exam Topic 3)
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 101
- (Exam Topic 3)
Which is NOT a SmartEvent component?

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

Answer: C

NEW QUESTION 106
- (Exam Topic 3)
What statement best describes the Proxy ARP feature for Manual NAT in R81.10?

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 108
- (Exam Topic 3)
Please choose the path to monitor the compliance status of the Check Point R81.10 based management.

A. Gateways & Servers --> Compliance View
B. Compliance blade not available under R81.10
C. Logs & Monitor --> New Tab --> Open compliance View
D. Security & Policies --> New Tab --> Compliance View

Answer: C

NEW QUESTION 109
- (Exam Topic 3)
Which tool is used to enable ClusterXL?

A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Answer: B

NEW QUESTION 112
- (Exam Topic 3)
Which file gives you a list of all security servers in use, including port number?

A. $FWDIR/conf/conf.conf
B. $FWDIR/conf/servers.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/conf/serversd.conf

Answer: C

NEW QUESTION 117
- (Exam Topic 3)
What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 118
- (Exam Topic 3)
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

NEW QUESTION 119
- (Exam Topic 3)
You can access the ThreatCloud Repository from:

A. R81.10 SmartConsole and Application Wiki
B. Threat Prevention and Threat Tools
C. Threat Wiki and Check Point Website
D. R81.10 SmartConsole and Threat Prevention

Answer: D

NEW QUESTION 123
- (Exam Topic 3)
Tom has connected to the R81 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 127

- (Exam Topic 3)
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 129
- (Exam Topic 3)
What command would show the API server status?

A. cpm status
B. api restart
C. api status
D. show api status

Answer: C

NEW QUESTION 131
- (Exam Topic 3)
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 R81.
What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81?

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 135
- (Exam Topic 3)
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. 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 140
- (Exam Topic 3)
Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows then as prioritized security events.

A. SmartMonitor
B. SmartView Web Application
C. SmartReporter
D. SmartTracker

Answer: B

NEW QUESTION 142
- (Exam Topic 3)
What is not a purpose of the deployment of Check Point API?

A. Execute an automated script to perform common tasks
B. Create a customized GUI Client for manipulating the objects database
C. Create products that use and enhance the Check Point solution
D. Integrate Check Point products with 3rd party solution

Answer: B

NEW QUESTION 143

- (Exam Topic 3)
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

A. ThreatWiki
B. Whitelist Files
C. AppWiki
D. IPS Protections

Answer: B

NEW QUESTION 144
- (Exam Topic 3)
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 148
- (Exam Topic 3)
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 24set static-route default nexthop gateway address 192.168.80.1 onsave config
B. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set 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 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 151
- (Exam Topic 3)
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 155
- (Exam Topic 3)
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 159
- (Exam Topic 3)
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 163
- (Exam Topic 3)
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 166
- (Exam Topic 3)
Which of the following is NOT an alert option?

A. SNMP
B. High alert
C. Mail
D. User defined alert

Answer: B

NEW QUESTION 167
- (Exam Topic 3)
When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related entries are present.
Which phase of the VPN negotiations has failed?

A. IKE Phase 1
B. IPSEC Phase 2
C. IPSEC Phase 1
D. IKE Phase 2

Answer: A

NEW QUESTION 168
- (Exam Topic 4)
What are the minimum open server hardware requirements for a Security Management Server/Standalone in R81?

A. 2 CPU cores, 4GB of RAM and 15GB of disk space
B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
C. 4 CPU cores, 8GB of RAM and 500GB of disk space
D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Answer: C

NEW QUESTION 170
- (Exam Topic 4)
What is the default size of NAT table fwx_alloc?

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

Answer: C

NEW QUESTION 173
- (Exam Topic 4)
The back end database for Check Point R81 Management uses:

A. DBMS
B. MongoDB
C. PostgreSQL
D. MySQL

Answer: C

NEW QUESTION 176
- (Exam Topic 4)
D18912E1457D5D1DDCBD40AB3BF70D5D
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 based and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

A. The connection is destined for a server within the network
B. The connection required a Security server
C. The packet is the second in an established TCP connection
D. The packets are not multicast

Answer: B

NEW QUESTION 178
- (Exam Topic 4)

How does the Anti-Virus feature of the Threat Prevention policy block traffic from infected websites?

A. By dropping traffic from websites identified through ThreatCloud Verification and URL Caching
B. By dropping traffic that is not proven to be from clean websites in the URL Filtering blade
C. By allowing traffic from websites that are known to run Antivirus Software on servers regularly
D. By matching logs against ThreatCloud information about the reputation of the website

Answer: D

NEW QUESTION 181
- (Exam Topic 4)
Which feature is NOT provided by all Check Point Mobile Access solutions?

A. Support for IPv6
B. Granular access control
C. Strong user authentication
D. Secure connectivity

Answer: A

Explanation:
Types of Solutions
All of Check Point's Remote Access solutions provide:

NEW QUESTION 184
- (Exam Topic 4)
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 188
- (Exam Topic 4)
Kurt is planning to upgrade his Security Management Server to R81.X. What is the lowest supported version of the Security Management he can upgrade from?

A. R76 Splat
B. R77.X Gaia
C. R75 Splat
D. R75 Gaia

Answer: D

NEW QUESTION 193
- (Exam Topic 4)
What are types of Check Point APIs available currently as part of R81.10 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 195
- (Exam Topic 4)
Which utility allows you to configure the DHCP service on Gaia from the command line?

A. ifconfig
B. dhcp_ofg
C. sysconfig
D. cpconfig

Answer: C

NEW QUESTION 199
- (Exam Topic 4)
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 202
- (Exam Topic 4)
After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?

A. You will find it in the home directory of your user account (e.
B. /home/admin/)
C. You can locate the file via SmartConsole > Command Line.
D. You have to launch the WebUI and go to "Config" -> "Export Config File" and specifiy the destination directory of your local file system.
E. You cannot locate the file in the file system since Clish does not have any access to the bash file system

Answer: A

NEW QUESTION 204
- (Exam Topic 4)
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 209
- (Exam Topic 4)
Which of the following is NOT a valid type of SecureXL template?

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

Answer: B

NEW QUESTION 214
- (Exam Topic 4)
Matt wants to upgrade his old Security Management server to R81.x using the Advanced Upgrade with Database Migration. What is one of the requirements for a successful upgrade?

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

Explanation:
https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/90083

NEW QUESTION 216
- (Exam Topic 4)
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 221
- (Exam Topic 4)
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: D

NEW QUESTION 222
- (Exam Topic 4)
Can Check Point and Third-party Gateways establish a certificate-based Site-to-Site VPN tunnel?

A. Yes, but they need to have a mutually trusted certificate authority
B. Yes, but they have to have a pre-shared secret key
C. No, they cannot share certificate authorities
D. No, Certificate based VPNs are only possible between Check Point devices

Answer: A

NEW QUESTION 226
- (Exam Topic 4)
There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A's interface issues were resolved and it became operational.
When it re-joins the cluster, will it become active automatically?

A. No, since 'maintain' current active cluster member' option on the cluster object properties is enabled by default.
B. No, since 'maintain' current active cluster member' option is enabled by default on the Global Properties.
C. Yes, since 'Switch to higher priority cluster member' option on the cluster object properties is enabled by default.
D. Yes, since 'Switch to higher priority cluster member' option is enabled by default on the Global Properties.

Answer: A

NEW QUESTION 229
- (Exam Topic 4)
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control
B. Threat Emulation
C. Anti-Virus
D. Advanced Networking Blade

Answer: B

NEW QUESTION 234
- (Exam Topic 4)
Which of the following is NOT an internal/native Check Point command?

A. fwaccel on
B. fw ct1 debug
C. tcpdump
D. cphaprob

Answer: C

NEW QUESTION 237
- (Exam Topic 4)
How many versions, besides the destination version, are supported in a Multi-Version Cluster Upgrade?

A. 1
B. 3
C. 2
D. 4

Answer: B

NEW QUESTION 242
- (Exam Topic 4)
What feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?

A. Specific VPN Communities
B. Remote Access VPN Switch
C. Mobile Access VPN Domain
D. Network Access VPN Domain

Answer: B

NEW QUESTION 246
- (Exam Topic 4)
Which of the following statements about SecureXL NAT Templates is true?

A. NAT Templates are generated to achieve high session rate for NA
B. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do

NAT without the expensive rulebase looku
C. These are enabled by default and work only if Accept Templates are enabled.
D. DROP Templates are generated to achieve high session rate for NA
E. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
F. These are disabled by default and work only if NAT Templates are disabled.
G. NAT Templates are generated to achieve high session rate for NA
H. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
I. These are disabled by default and work only if Accept Templates are disabled.
J. ACCEPT Templates are generated to achieve high session rate for NA
K. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase looku
L. These are disabled by default and work only if NAT Templates are disabled.

Answer: A

NEW QUESTION 247
- (Exam Topic 4)
What should the admin do in case the Primary Management Server is temporary down?

A. Use the VIP in SmartConsole you always reach the active Management Server.
B. The Secondary will take over automatically Change the IP in SmartConsole to logon to the private IP of the Secondary Management Server.
C. Run the 'promote_util' to activate the Secondary Management server
D. Logon with SmartConsole to the Secondary Management Server and choose "Make Active' under Actions in the HA Management Menu

Answer: A

NEW QUESTION 252
- (Exam Topic 4)
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

NEW QUESTION 253
- (Exam Topic 4)
When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

A. Syslog
B. SNMPTrap
C. Block Source
D. Mail

Answer: B

NEW QUESTION 255
- (Exam Topic 4)
Bob is asked by Alice to disable the SecureXL mechanism temporary tor further diagnostic by their Check Point partner. Which of the following Check Point Command is true:

A. fwaccel suspend
B. fwaccel standby
C. fwaccel off
D. fwaccel templates

Answer: C

NEW QUESTION 259
- (Exam Topic 4)
What is the default shell of Gaia CLI?

A. Monitor
B. CLI.sh
C. Read-only
D. Bash

Answer: B

NEW QUESTION 264
- (Exam Topic 4)

What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

A. Idle <20%
B. USR <20%
C. SYS <20%
D. Wait <20%

Answer: A

NEW QUESTION 266
- (Exam Topic 4)
True or False: In R81, more than one administrator can login to the Security Management Server with write permission at the same time.

A. False, this feature has to be enabled in the Global Properties.
B. True, every administrator works in a session that is independent of the other administrators.
C. True, every administrator works on a different database that is independent of the other administrators.
D. False, only one administrator can login with write permission.

Answer: B

NEW QUESTION 270
- (Exam Topic 4)
DLP and Geo Policy are examples of what type of Policy?

A. Standard Policies
B. Shared Policies
C. Inspection Policies
D. Unified Policies

Answer: B

NEW QUESTION 273
- (Exam Topic 4)
What is Dynamic Balancing?

A. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput
B. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load
C. It is a new feature that is capable of dynamically reserve the amount of Hash kernel memory to reflect the resource usage necessary for maximizing the session rate.
D. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces

Answer: B

NEW QUESTION 274
- (Exam Topic 4)
To find records in the logs that shows log records from the Application & URL Filtering Software Blade where traffic was dropped, what would be the query syntax?

A. blada: application control AND action:drop
B. blade."application control AND action;drop
C. (blade: application control AND action;drop)
D. blade;"application control AND action:drop

Answer: D

NEW QUESTION 277
- (Exam Topic 4)
According to the policy installation flow the transfer state (CPTA) is responsible for the code generated by the FWM. On the Security Gateway side a process receives them and first stores them Into a temporary directory. Which process is true for receiving these Tiles;

A. FWD
B. CPD
C. FWM
D. RAD

Answer: A

NEW QUESTION 281
- (Exam Topic 4)
Which one is not a valid Package Option In the Web GUI for CPUSE?

A. Clean Install
B. Export Package
C. Upgrade
D. Database Conversion to R81.10 only

Answer: B

NEW QUESTION 284
- (Exam Topic 4)
Which of the following processes pulls the application monitoring status from gateways?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 4)
While using the Gaia CLI. what is the correct command to publish changes to the management server?

A. json publish
B. mgmt publish
C. mgmt_cli commit
D. commit

Answer: B

NEW QUESTION 288
- (Exam Topic 4)
Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:

A. ReverseCLIProxy
B. ReverseProxyCLI
C. ReverseProxy
D. ProxyReverseCLI

Answer: C

NEW QUESTION 291
- (Exam Topic 4)
When performing a minimal effort upgrade, what will happen to the network traffic?

A. All connections that were Initiated before the upgrade will be dropped, causing network downtime.
B. All connections that were initiated before the upgrade will be handled by the active gateway
C. All connections that were initiated before the upgrade will be handled normally
D. All connections that were initiated before the upgrade will be handled by the standby gateway

Answer: B

NEW QUESTION 292
- (Exam Topic 4)
What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

A. CPUSE offline upgrade only
B. Advanced upgrade or CPUSE offline upgrade
C. Advanced Upgrade only
D. SmartUpdate offline upgrade

Answer: B

NEW QUESTION 293
- (Exam Topic 4)
What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

A. test_connectivity_ad –d <domain>
B. test_ldap_connectivity –d <domain>
C. test_ad_connectivity –d <domain>
D. ad_connectivity_test –d <domain>

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/
CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/ CP_R81.30_CLI_ReferenceGuide/200877

NEW QUESTION 295
- (Exam Topic 4)
You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

A. fw unloadlocal
B. fw unloadpolicy
C. fwm unload local
D. fwm unload policy

Answer: A

NEW QUESTION 298
- (Exam Topic 4)
What are possible Automatic Reactions in SmartEvent?

A. Mai
B. SNMP Trap, Block Sourc
C. Block Event Activity, External Script
D. Web Mai
E. Block Destination, SNMP Tra
F. SmartTask
G. Web Mail, Block Servic
H. SNMP Tra
I. SmartTask, Geo Protection
J. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

Answer: A

NEW QUESTION 301
- (Exam Topic 4)
What command is used to manually failover a cluster during a zero downtime upgrade?

A. set cluster member down
B. cpstop
C. clusterXL_admin down
D. set clusterXL down

Answer: C

NEW QUESTION 305
- (Exam Topic 4)
In the Check Point Security Management Architecture, which component(s) can store logs?

A. SmartConsole
B. Security Management Server and Security Gateway
C. Security Management Server
D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 308
- (Exam Topic 4)
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 312
- (Exam Topic 4)
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 315
- (Exam Topic 4)
CoreXL is NOT supported when one of the following features is enabled: (Choose three)

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

Answer: ACD

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

NEW QUESTION 316
.....

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

156-315.81 Practice Exam Features:

* 156-315.81 Questions and Answers Updated Frequently

* 156-315.81 Practice Questions Verified by Expert Senior Certified Staff

* 156-315.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-315.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 156-315.81 Practice Test Here