CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

NEW QUESTION 1
- (Exam Topic 1)
Which of the following is a new R81 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 2
- (Exam Topic 1)
How can SmartView application accessed?

A. http://<Security Management IP Address>/smartview
B. http://<Security Management IP Address>:4434/smartview/
C. https://<Security Management IP Address>/smartview/
D. https://<Security Management host name>:4434/smartview/

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) ______ or _______ action for the file types.

A. Inspect/Bypass
B. Inspect/Prevent
C. Prevent/Bypass
D. Detect/Bypass

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
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

NEW QUESTION 5
- (Exam Topic 1)
Which command collects diagnostic data for analyzing customer setup remotely?

A. cpinfo
B. migrate export
C. sysinfo
D. cpview

Answer: A

Explanation:
CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).
The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

NEW QUESTION 6
- (Exam Topic 1)
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

NEW QUESTION 7

- (Exam Topic 1)
What is the least amount of CPU cores required to enable CoreXL?

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

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
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 9
- (Exam Topic 1)
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

NEW QUESTION 10
- (Exam Topic 1)
Fill in the blank: The R81 feature ______ permits blocking specific IP addresses for a specified time period.

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

Answer: C

Explanation:
Suspicious Activity Rules Solution
Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).
The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.

NEW QUESTION 10
- (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 15
- (Exam Topic 1)
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 16
- (Exam Topic 1)
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 18
- (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 23
- (Exam Topic 1)
There are 4 ways to use the Management API for creating host object with R81 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

NEW QUESTION 28
- (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 29
- (Exam Topic 1)
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

NEW QUESTION 31
- (Exam Topic 1)
Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 33
- (Exam Topic 1)
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 34
- (Exam Topic 1)
Tom has been tasked to install Check Point R81 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

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

Answer: C

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

NEW QUESTION 36
- (Exam Topic 1)
Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid
B. Accept-Charset
C. Proxy-Authorization
D. Application

Answer: C

NEW QUESTION 40
- (Exam Topic 1)
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

NEW QUESTION 45
- (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 49
- (Exam Topic 1)
Which of the following statements is TRUE about R81 management plug-ins?

A. The plug-in is a package installed on the Security Gateway.
B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Answer: C

NEW QUESTION 50
- (Exam Topic 1)
Where you can see and search records of action done by R81 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 55
- (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 60
- (Exam Topic 1)
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 62
- (Exam Topic 2)
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 64
- (Exam Topic 2)
Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

A. cphaprob stat
B. cphaprob –a if
C. cphaprob –l list
D. cphaprob all show stat

Answer: D

NEW QUESTION 69
- (Exam Topic 2)
What are the blades of Threat Prevention?

A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
C. IPS, AntiVirus, AntiBot
D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

Answer: D

NEW QUESTION 70
- (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 71
- (Exam Topic 2)
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.

NEW QUESTION 74
- (Exam Topic 2)
Which GUI client is supported in R81?

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

Answer: C

NEW QUESTION 75
- (Exam Topic 2)
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 80
- (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 81
- (Exam Topic 2)
Which of the following will NOT affect acceleration?

A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)

Answer: B

NEW QUESTION 86
- (Exam Topic 2)
What is the protocol and port used for Health Check and State Synchronization in ClusterXL?

A. CCP and 18190
B. CCP and 257
C. CCP and 8116
D. CPC and 8116

Answer: C

NEW QUESTION 88
- (Exam Topic 2)
For Management High Availability, which of the following is NOT a valid synchronization status?

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

Answer: B

NEW QUESTION 91
- (Exam Topic 2)
Which of the following is NOT a type of Check Point API available in R81.x?

A. Identity Awareness Web Services
B. OPSEC SDK
C. Mobile Access
D. Management

Answer:

C

NEW QUESTION 92
- (Exam Topic 2)
What is the purpose of extended master key extension/session hash?

A. UDP VOIP protocol extension
B. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication
C. Special TCP handshaking extension
D. Supplement DLP data watermark

Answer: B

NEW QUESTION 93
- (Exam Topic 2)
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 94
- (Exam Topic 2)
You have existing dbedit scripts from R77. Can you use them with R81.10?

A. dbedit is not supported in R81.10
B. dbedit is fully supported in R81.10
C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
D. dbedit scripts are being replaced by mgmt_cli in R81.10

Answer: D

NEW QUESTION 99
- (Exam Topic 2)
What is a best practice before starting to troubleshoot using the “fw monitor” tool?

A. Run the command: fw monitor debug on
B. Clear the connections table
C. Disable CoreXL
D. Disable SecureXL

Answer: D

NEW QUESTION 101
- (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 102
- (Exam Topic 2)
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 106
- (Exam Topic 2)
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 111
- (Exam Topic 2)
What processes does CPM control?

A. Object-Store, Database changes, CPM Process and web-services
B. web-services, CPMI process, DLEserver, CPM process
C. DLEServer, Object-Store, CP Process and database changes
D. web_services, dle_server and object_Store

Answer: D

NEW QUESTION 112
- (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 115
- (Exam Topic 2)
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 120
- (Exam Topic 2)
Which Remote Access Client does not provide an Office-Mode Address?

A. SecuRemote
B. Endpoint Security Suite
C. Endpoint Security VPN
D. Check Point Mobile

Answer: A

NEW QUESTION 123
- (Exam Topic 2)
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 126
- (Exam Topic 2)

Which directory below contains log files?

A. /opt/CPSmartlog-R81/log
B. /opt/CPshrd-R81/log
C. /opt/CPsuite-R81/fw1/log
D. /opt/CPsuite-R81/log

Answer: C

NEW QUESTION 131
- (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 133
- (Exam Topic 2)
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

NEW QUESTION 138
- (Exam Topic 2)
When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?

A. IP
B. SIC
C. NAT
D. FQDN

Answer: C

NEW QUESTION 140
- (Exam Topic 2)
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 143
- (Exam Topic 2)
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 146
- (Exam Topic 2)
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 147
- (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 150
- (Exam Topic 2)
You want to store the GAIA configuration in a file for later reference. What command should you use?

A. write mem <filename>
B. show config –f <filename>
C. save config –o <filename>
D. save configuration <filename>

Answer: D

NEW QUESTION 152
- (Exam Topic 2)
Which web services protocol is used to communicate to the Check Point R81 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 153
- (Exam Topic 2)
Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 156
- (Exam Topic 2)
Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.10 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 158
- (Exam Topic 2)
Automation and Orchestration differ in that:

A. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
B. Automation involves the process of coordinating an exchange of information through web service interactions such as XML and JSON, but orchestration does not involve processes.
C. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and puts them all together into a process workflow.
D. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.

Answer: A

NEW QUESTION 161
- (Exam Topic 2)
Which one of the following is true about Threat Emulation?

A. Takes less than a second to complete
B. Works on MS Office and PDF files only

C. Always delivers a file
D. Takes minutes to complete (less than 3 minutes)

Answer: D

NEW QUESTION 162
- (Exam Topic 2)
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 165
- (Exam Topic 2)
After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

A. cvpnd_restart
B. cvpnd_restart
C. cvpnd restart
D. cvpnrestart

Answer: B

NEW QUESTION 167
- (Exam Topic 2)
The following command is used to verify the CPUSE version:

A. HostName:0>show installer status build
B. [Expert@HostName:0]#show installer status
C. [Expert@HostName:0]#show installer status build
D. HostName:0>show installer build

Answer: A

NEW QUESTION 168
- (Exam Topic 3)
Fill in the blank: Identity Awareness AD-Query is using the Microsoft _______ API to learn users from AD.

A. WMI
B. Eventvwr
C. XML
D. Services.msc

Answer: A

NEW QUESTION 169
- (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 171
- (Exam Topic 3)
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

NEW QUESTION 176
- (Exam Topic 3)
What is the Implicit Clean-up Rule?

A. A setting is defined in the Global Properties for all policies.
B. A setting that is configured per Policy Layer.
C. Another name for the Clean-up Rule.
D. Automatically created when the Clean-up Rule is defined.

Answer: C

NEW QUESTION 179
- (Exam Topic 3)
You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.
What must you do to get SIC to work?

A. Remove Geo-Protection, as the IP-to-country database is updated externally, and you have no control of this.
B. Create a rule at the top in the Sydney firewall to allow control traffic from your network
C. Nothing - Check Point control connections function regardless of Geo-Protection policy
D. Create a rule at the top in your Check Point firewall to bypass the Geo-Protection

Answer: C

NEW QUESTION 182
- (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 184
- (Exam Topic 3)
Fill in the blank: The “fw monitor” tool can be best used to troubleshoot ______.

A. AV issues
B. VPN errors
C. Network traffic issues
D. Authentication issues

Answer: C

Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal? eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

NEW QUESTION 185
- (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 190
- (Exam Topic 3)
One of major features in R81 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

A. A lock icon shows that a rule or an object is locked and will be available.
B. AdminA and AdminB are editing the same rule at the same time.
C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is ______ .

A. Sent to the Internal Certificate Authority.
B. Sent to the Security Administrator.
C. Stored on the Security Management Server.
D. Stored on the Certificate Revocation List.

Answer: D

NEW QUESTION 198
- (Exam Topic 3)
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 203
- (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 207
- (Exam Topic 3)
What kind of information would you expect to see using the sim affinity command?

A. The VMACs used in a Security Gateway cluster
B. The involved firewall kernel modules in inbound and outbound packet chain
C. Overview over SecureXL templated connections
D. Network interfaces and core distribution used for CoreXL

Answer: D

NEW QUESTION 212
- (Exam Topic 3)
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 216
- (Exam Topic 3)
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 217
- (Exam Topic 3)
Which blades and or features are not supported in R81?

A. SmartEvent Maps
B. SmartEvent
C. Identity Awareness
D. SmartConsole Toolbars

Answer: A

NEW QUESTION 218
- (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 220
- (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 221
- (Exam Topic 3)
Which Check Point feature enables application scanning and the detection?

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

Answer: B

NEW QUESTION 224
- (Exam Topic 3)
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment

Answer: D

NEW QUESTION 227
- (Exam Topic 3)
What is the SandBlast Agent designed to do?

A. Performs OS-level sandboxing for SandBlast Cloud architecture
B. Ensure the Check Point SandBlast services is running on the end user’s system
C. If malware enters an end user’s system, the SandBlast Agent prevents the malware from spreading with the network
D. Clean up email sent with malicious attachments

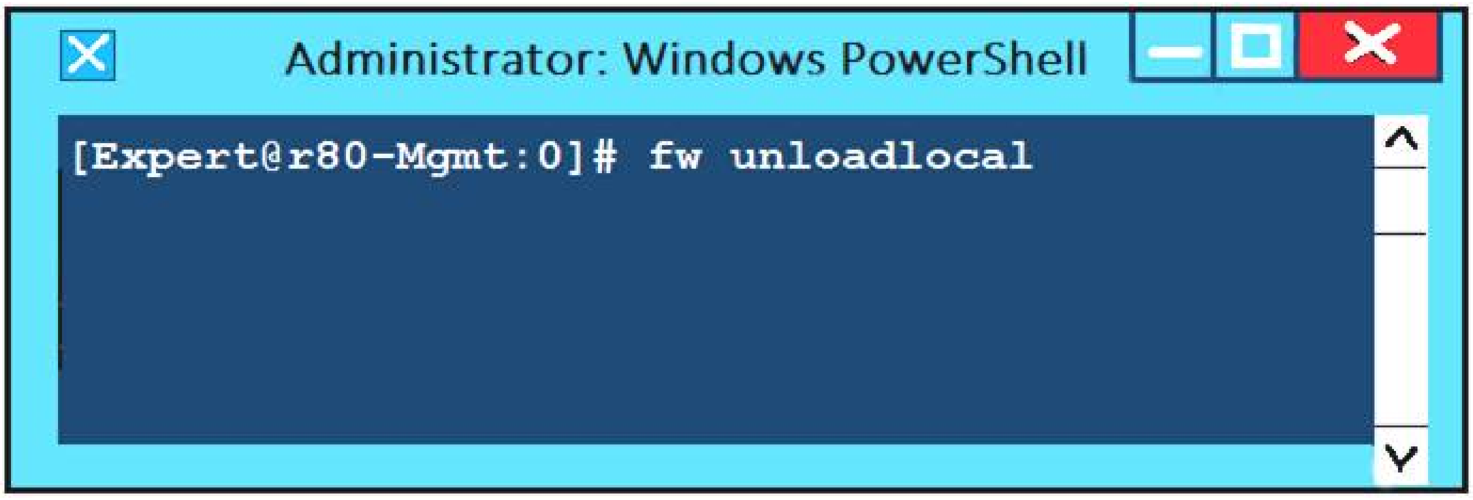
Answer: C

NEW QUESTION 229
- (Exam Topic 3)
You want to verify if your management server is ready to upgrade to R81.10. What tool could you use in this process?

A. migrate export
B. upgrade_tools verify
C. pre_upgrade_verifier
D. migrate import

Answer: C

NEW QUESTION 230
- (Exam Topic 3)
What will be the effect of running the following command on the Security Management Server?



```
[Expert@r80-Mgmt:0]# fw unloadlocal
```

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

Answer: A

NEW QUESTION 234
- (Exam Topic 3)
In ClusterXL Load Sharing Multicast Mode:

A. only the primary member received packets sent to the cluster IP address
B. only the secondary member receives packets sent to the cluster IP address
C. packets sent to the cluster IP address are distributed equally between all members of the cluster
D. every member of the cluster received all of the packets sent to the cluster IP address

Answer: D

NEW QUESTION 238
- (Exam Topic 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 Stateful Mode configuration, chain modules marked with _______ will not apply.

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

Answer: D

NEW QUESTION 240
- (Exam Topic 3)
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 243
- (Exam Topic 3)
What is the valid range for VRID value in VRRP configuration?

A. A.-1 - 254B.1 - 255C.0 - 254D.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 246
- (Exam Topic 3)
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 249
- (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 250
- (Exam Topic 3)
What are the methods of SandBlast Threat Emulation deployment?

A. Cloud, Appliance and Private
B. Cloud, Appliance and Hybrid
C. Cloud, Smart-1 and Hybrid
D. Cloud, OpenServer and Vmware

Answer: A

NEW QUESTION 253
- (Exam Topic 4)
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsive, which if these steps should NOT be performed:

A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
B. Change the Standby Security Management Server to Active.
C. Change the Active Security Management Server to Standby.
D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 255
- (Exam Topic 4)
When Configuring Endpoint Compliance Settings for Applications and Gateways within Mobile Access, which of the three approaches will allow you to configure individual policies for each application?

A. Basic Approach
B. Strong Approach
C. Very Advanced Approach
D. Medium Approach

Answer: C

NEW QUESTION 258
- (Exam Topic 4)
If SecureXL is disabled which path is used to process traffic?

A. Passive path
B. Medium path
C. Firewall path
D. Accelerated path

Answer: C

NEW QUESTION 263
- (Exam Topic 4)
After finishing installation admin John likes to use top command in expert mode. John has to set the
expert-password and was able to use top command. A week later John has to use the top command again, He detected that the expert password is no longer valid. What is the most probable reason for this behavior?

A. “write memory” was not issued on clish
B. changes are only possible via SmartConsole
C. “save config” was not issued in expert mode
D. “save config” was not issued on clish

Answer: D

NEW QUESTION 266
- (Exam Topic 4)
Which command lists firewall chain?

A. fwctl chain
B. fw list chain
C. fw chain module
D. fw tab -t chainmod

Answer: A

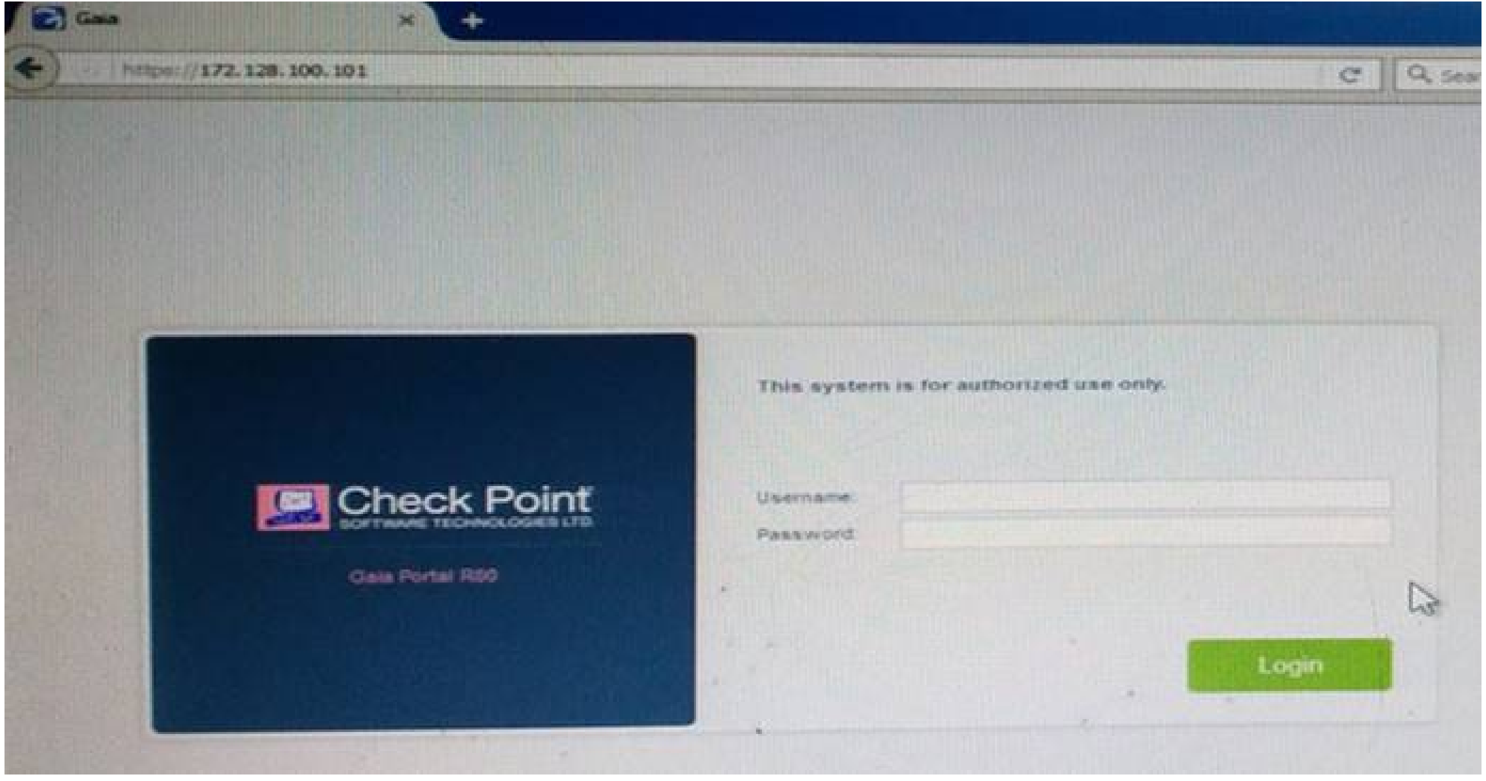
Explanation:
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION 268
- (Exam Topic 4)
A user complains that some Internet resources are not available. The Administrator is having issues seeing it packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?

A. run fw unloadlocal" on the relevant gateway and check the ping again
B. run "cpstop" on the relevant gateway and check the ping again
C. run ''fw log" on the relevant gateway
D. run ''fw ctl zdebug drop" on the relevant gateway

Answer: D

NEW QUESTION 271
- (Exam Topic 4)
Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



This system is for authorized use only.

A. set web ssl-port <new port number>
B. set Gaia-portal port <new port number>
C. set Gaia-portal https-port <new port number>
D. set web https-port <new port number>

Answer: A

NEW QUESTION 276
- (Exam Topic 4)
What is the SOLR database for?

A. Used for full text search and enables powerful matching capabilities
B. Writes data to the database and full text search
C. Serves GUI responsible to transfer request to the DLE server
D. Enables powerful matching capabilities and writes data to the database

Answer: A

NEW QUESTION 280
- (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 284
- (Exam Topic 4)
Bob works for a big security outsourcing provider company and as he receives a lot of change requests per day he wants to use for scripting daily tasks the API services (torn Check Point for the GAIA API. Firstly he needs to be aware if the API services are running for iheGAIA operating system. Which of the following Check Point Command is true:

A. gala_dlish status
B. status gaiaapi
C. api_gala status
D. gala_api status

Answer: A

NEW QUESTION 286
- (Exam Topic 4)
Which of the following Check Point commands is true to enable Multi-Version Cluster (MVC)?

A. Check Point Security Management HA (Secondary): set cluster member mvc on
B. Check Point Security Gateway Only: set cluster member mvc on
C. Check Point Security Management HA (Primary): set cluster member mvc on
D. Check Point Security Gateway Cluster Member: set cluster member mvc on

Answer: D

NEW QUESTION 288
- (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 291
- (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 294
- (Exam Topic 4)
You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.
What is the first step to run management API commands on GAIA's shell?

A. mgmt_admin@teabag > id.txt
B. mgmt_login
C. login user admin password teabag
D. mgmt_cli login user “admin” password “teabag” > id.txt

Answer: B

NEW QUESTION 295
- (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 298
- (Exam Topic 4)

When defining QoS global properties, which option below is not valid?

A. Weight
B. Authenticated timeout
C. Schedule
D. Rate

Answer: D

NEW QUESTION 301
- (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 306
- (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 310
- (Exam Topic 4)
Which upgrade method you should use upgrading from R80.40 to R81.10 to avoid any downtime?

A. Zero Downtime Upgrade (ZDU)
B. Connectivity Upgrade (CU)
C. Minimal Effort Upgrade (ME)
D. Multi-Version Cluster Upgrade (MVC)

Answer: D

NEW QUESTION 313
- (Exam Topic 4)
John detected high load on sync interface. Which is most recommended solution?

A. For FTP connections – do not sync
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 314
- (Exam Topic 4)
What is the purpose of the command "ps aux | grep twd"?

A. You can check the Process ID and the processing time of the twd process.
B. You can convert the log file into Post Script format.
C. You can list all Process IDs for all running services.
D. You can check whether the IPS default setting is set to Detect or Prevent mode

Answer: A

NEW QUESTION 318
- (Exam Topic 4)
You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways

A. action:"Key Install" AND 1.1.1.1 AND Main Mode
B. action:"Key Install- AND 1.1.1.1 ANDQuick Mode
C. Blade:"VPN" AND VPN-Stores AND Main Mode
D. Blade:"VPN" AND VPN-Stores AND Quick Mode

Answer: C

NEW QUESTION 323
- (Exam Topic 4)
What is a possible command to delete all of the SSH connections of a gateway?

A. fw sam -I dport 22
B. fw ctl conntab -x -dpott=22
C. fw tab -t connections -x -e 00000016
D. fwaccel dos config set dport ssh

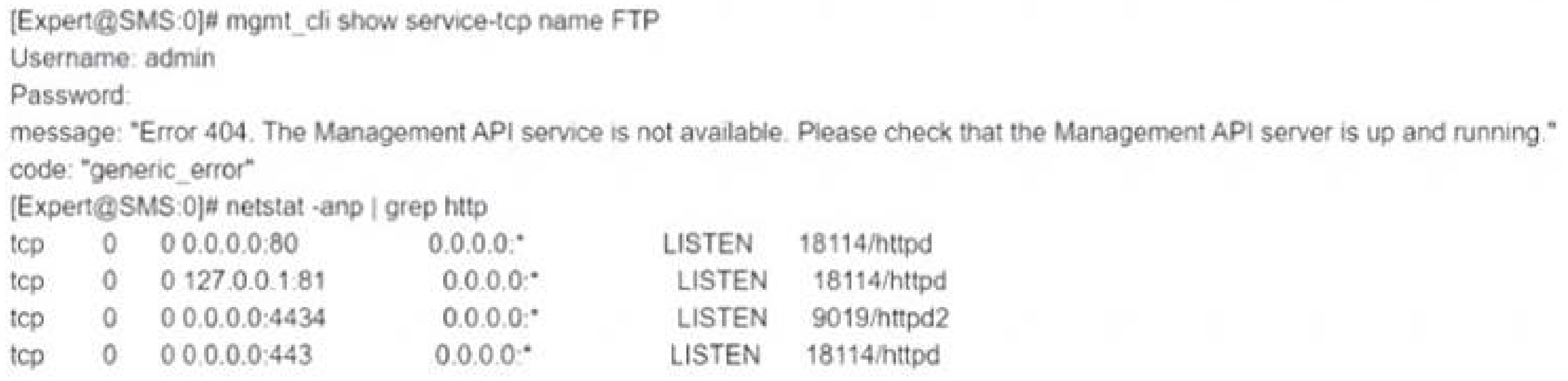
Answer: A

NEW QUESTION 325
- (Exam Topic 4)
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 329
- (Exam Topic 4)
The admin is connected via ssh lo the management server. He wants to run a mgmt_dl command but got a Error 404 message. To check the listening ports on the management he runs netstat with the results shown below. What can be the cause for the issue?



```
[Expert@SMS:0]# mgmt_cli show service-tcp name FTP
Username: admin
Password:
message: "Error 404. The Management API service is not available. Please check that the Management API server is up and running."
code: "generic_error"
[Expert@SMS:0]# netstat -anp | grep http
tcp     0     0 0.0.0.0:80           0.0.0.0:*          LISTEN     18114/httpd
tcp     0     0 127.0.0.1:81          0.0.0.0:*          LISTEN     18114/httpd
tcp     0     0 0.0.0.0:4434          0.0.0.0:*          LISTEN     9019/httpd2
tcp     0     0 0.0.0.0:443          0.0.0.0:*          LISTEN     18114/httpd
```

A. Wrong Management API Access setting^for Ihe client IP To correct it go to SmartConsole / Management & Settings / Blades / Management API and press "Advanced Settings..' and choose GUI clients or ALL IP's.
B. The API didn't run on the default port check it with api status' and add '-port 4434' to the mgmt_clt command.
C. The management permission in the user profile is mrssin
D. Go to SmartConsole / Management & Settings I Permissions & Administrators / Permission Profile
E. Select the profile of the user and enable 'Management API Login' under Management Permissions
F. The API is not running, the services shown by netstat are the gaia service
G. To start the API run 'api start'

Answer: A

NEW QUESTION 334
- (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 338
- (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 340
- (Exam Topic 4)
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. Run cprestart from clish
B. After upgrading the hardware, increase the number of kernel instances using cpconfig
C. Administrator does not need to perform any tas
D. Check Point will make use of the newly installed CPU and Cores
E. Hyperthreading must be enabled in the bios to use CoreXL

Answer: B

NEW QUESTION 343
- (Exam Topic 4)
By default how often updates are checked when the CPUSE Software Updates Policy is set to Automatic?

A. Six times per day
B. Seven times per day
C. Every two hours
D. Every three hours

Answer: D

Explanation:

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/
html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

NEW QUESTION 345
- (Exam Topic 4)
Which Correction mechanisms are available with ClusterXL under R81.10?

A. Correction Mechanisms are only available of Maestro Hyperscale Orchestrators
B. Pre-Correction and SDF (Sticky Decision Function)
C. SDF (Sticky Decision Function) and Flush and ACK
D. Dispatcher (Early Correction) and Firewall (Late Correction)

Answer: C

NEW QUESTION 348
- (Exam Topic 4)
SecureXL is able to accelerate the Connection Rate using templates. Which attnbutes are used in the template to identify the connection?

A. Source address . Destination addres
B. Source Port, Destination port
C. Source address . Destination addres
D. Destination port
E. Source address . Destination addres
F. Destination por
G. Pro^col
H. Source address . Destination addres
I. Source Port, Destination por
J. Protocol

Answer: D

NEW QUESTION 352
- (Exam Topic 4)
The Compliance Blade allows you to search for text strings in many windows and panes, to search for a value in a field, what would your syntax be?

A. field_name:string
B. name field:string
C. name_field:string
D. field name:string

Answer: A

NEW QUESTION 356
- (Exam Topic 4)

The WebUI offers several methods for downloading hotfixes via CPUSE except:

A. Automatic
B. Force override
C. Manually
D. Scheduled

Answer: B

NEW QUESTION 358
- (Exam Topic 4)
What is the correct order of the default “fw monitor” inspection points?

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

Answer: C

NEW QUESTION 361
- (Exam Topic 4)
When users connect to the Mobile Access portal they are unable to open File Shares. Which log file would you want to examine?

A. cvpnd.elg
B. httpd.elg
C. vpnd.elg
D. fw.elg

Answer: A

NEW QUESTION 363
- (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 366
- (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 367
- (Exam Topic 4)
What is the default shell for the command line interface?

A. Expert
B. Clish
C. Admin
D. Normal

Answer: B

Explanation:
The default shell of the CLI is called clish References:

NEW QUESTION 370
- (Exam Topic 4)
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

A. Use Multi-Domain Management Server.
B. Choose different setting for log storage and SmartEvent db
C. Install Management and SmartEvent on different machines.
D. it is not possible.

Answer: C

NEW QUESTION 372
- (Exam Topic 4)
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 376
- (Exam Topic 4)
Bob has finished io setup provisioning a secondary security management server. Now he wants to check if the provisioning has been correct. Which of the following Check Point command can be used to check if the security management server has been installed as a primary or a secondary security management server?

A. cpprod_util MgmtlsPrimary
B. cpprod_util FwlsSecondary
C. cpprod_util MgmtlsSecondary
D. cpprod_util FwlsPrimary

Answer: A

NEW QUESTION 378
- (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 382
- (Exam Topic 4)
When synchronizing clusters, which of the following statements is FALSE?

A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
B. Only cluster members running on the same OS platform can be synchronized.
C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.

Answer: D

NEW QUESTION 383
- (Exam Topic 4)
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: D

NEW QUESTION 386
- (Exam Topic 4)
By default, the R81 web API uses which content-type in its response?

A. Java Script
B. XML
C. Text
D. JSON

Answer: D

NEW QUESTION 390
- (Exam Topic 4)
How many users can have read/write access in Gaia at one time?

A. Infinite
B. One
C. Three
D. Two

Answer: B

NEW QUESTION 394
- (Exam Topic 4)
The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?

A. In expert mode run #netstat -tulnp | grep httpd to see if httpd is up and to get the port numbe
B. In dish run >show web daemon-enable to see if the web daemon is enabled.
C. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in us
D. In expert mode run #netstat -anp | grep httpd to see if the httpd is up
E. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in us
F. In expert mode run #netstat -anp | grep httpd2 to see if the httpd2 is up
G. In expert mode run #netstat -tulnp | grep httpd2 to see if httpd2 is up and to get the port numbe
H. In dish run >show web daemon-enable to see if the web daemon is enabled.

Answer: C

NEW QUESTION 399
- (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 404
- (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 406
- (Exam Topic 4)
You want to gather data and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

A. Check Point Capsule Cloud
B. Sandblast Mobile Protect
C. SecuRemote
D. SmartEvent Client Info

Answer: B

Explanation:
SandBlast Mobile Protect is a lightweight app for iOS and Android™ that gathers data and helps analyze threats to devices in your environment.
https://www.checkpoint.com/downloads/products/how-sandblast-mobile-works-solution-brief.pdf

NEW QUESTION 409
- (Exam Topic 4)
SmartEvent Security Checkups can be run from the following Logs and Monitor activity:

A. Reports
B. Advanced
C. Checkups
D. Views

Answer: A

NEW QUESTION 414
- (Exam Topic 4)
What are the available options for downloading Check Point hotfixes in Gala WebUI (CPUSE)?

A. Manually, Scheduled, Automatic
B. Manually, Automatic, Disabled
C. Manually, Scheduled, Disabled
D. Manually, Scheduled, Enabled

Answer: A

Explanation:

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/
html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

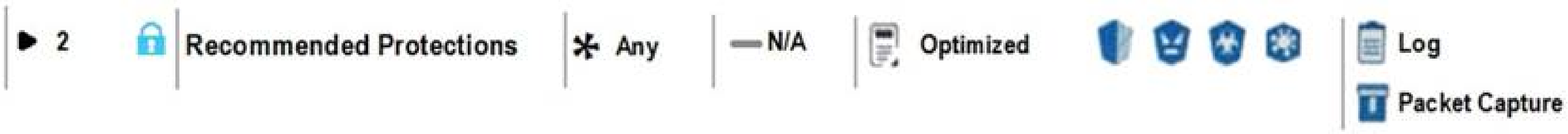
NEW QUESTION 419
- (Exam Topic 4)
Which of the following is a task of the CPD process?

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: B

Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12496.htm

NEW QUESTION 424
- (Exam Topic 4)
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



2 Recommended Protections | Any | N/A | Optimized | Log, Packet Capture

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

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_

NEW QUESTION 429
- (Exam Topic 4)
What component of Management is used tor indexing?

A. DBSync
B. API Server
C. fwm
D. SOLR

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Multi-DomainSecurityManag

NEW QUESTION 434
- (Exam Topic 4)
Which of the following is NOT an attribute of packet acceleration?

A. Source address
B. Protocol
C. Destination port
D. VLAN Tag

Answer: D

NEW QUESTION 438
- (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 441
- (Exam Topic 4)
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 442
- (Exam Topic 4)
Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

A. $FWDIR/conf/client.scv
B. $CPDIR/conf/local.scv
C. $CPDIR/conf/client.svc
D. $FWDIR/conf/local.scv

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG

NEW QUESTION 447
- (Exam Topic 4)
Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

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

Answer: D

NEW QUESTION 450
- (Exam Topic 4)
Which two Cluster Solutions are available under R81.10?

A. ClusterXL and NSRP
B. VRRPandHSRP
C. VRRP and IP Clustering
D. ClusterXL and VRitP

Answer: D

NEW QUESTION 452
- (Exam Topic 4)
If a “ping”-packet is dropped by FW1 Policy –on how many inspection Points do you see this packet in “fw monitor”?

A. “i", “I” and “o”
B. I don’t see it in fw monitor
C. “i" only
D. “i" and “I”

Answer: C

NEW QUESTION 453
- (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 457
- (Exam Topic 4)
Fill in the blank: Authentication rules are defined for ______ .

A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database

Answer: A

NEW QUESTION 460
- (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 464
- (Exam Topic 4)
Which is the command to identify the NIC dnver before considering about the employment of the Multi-Queue feature?

A. show interface eth0 mq
B. ethtool A eth0
C. ifconfig -i eth0 verbose
D. ip show Int eth0

Answer: A

NEW QUESTION 466
- (Exam Topic 4)
By default, which port does the WebUI listen on?

A. 80
B. 4434
C. 443
D. 8080

Answer: C

NEW QUESTION 471
- (Exam Topic 4)
What are the two types of tests when using the Compliance blade?

A. Policy-based tests and Global properties
B. Global tests and Object-based tests
C. Access Control policy analysis and Threat Prevention policy analysis
D. Tests conducted based on the loC XMfcfile and analysis of SOLR documents

Answer: D

NEW QUESTION 473
......