CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

NEW QUESTION 1
- (Exam Topic 1)
SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?

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

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
Which of these statements describes the Check Point ThreatCloud?

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

Answer: D

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
What is true about the IPS-Blade?

A. In R81, IPS is managed by the Threat Prevention Policy
B. In R81, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. In R81, IPS Exceptions cannot be attached to "all rules"
D. In R81, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
Which command is used to set the CCP protocol to Multicast?

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

Answer: B

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 1)
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don’t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw ctl multik dynamic_dispatching on
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. fw ctl multik pq enable

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
Which features are only supported with R81.10 Gateways but not R77.x?

A. Access Control policy unifies the Firewall, Application Control & URL Filtering, Data Awareness, and Mobile Access Software Blade policies.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. The rule base can be built of layers, each containing a set of the security rule
D. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
E. Time object to a rule to make the rule active only during specified times.

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
Fill in the blank: The R81 utility fw monitor is used to troubleshoot .

A. User data base corruption
B. LDAP conflicts
C. Traffic issues
D. Phase two key negotiations

Answer: C

Explanation:
Check Point’s FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

NEW QUESTION 14
- (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 18
- (Exam Topic 1)
Which command can you use to verify the number of active concurrent connections?

A. fw conn all
B. fw ctl pstat
C. show all connections

D. show connections

Answer: B

NEW QUESTION 22
- (Exam Topic 1)
Which TCP-port does CPM process listen to?

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

Answer: D

NEW QUESTION 24
- (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 27
- (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 30
- (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 34
- (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 38
- (Exam Topic 1)
What Factor preclude Secure XL Templating?

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

Answer:

A

NEW QUESTION 42
- (Exam Topic 1)
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _____.

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

Answer: A

NEW QUESTION 43
- (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 48
- (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 52
- (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 55
- (Exam Topic 1)
Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

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

Answer: B

NEW QUESTION 59
- (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 60
- (Exam Topic 1)
Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 65
- (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 70
- (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 74
- (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 75
- (Exam Topic 1)
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated management console. It empowers the migration from legacy Client-side logic to Server-side logic. The cpm process:

A. Allow GUI Client and management server to communicate via TCP Port 19001
B. Allow GUI Client and management server to communicate via TCP Port 18191
C. Performs database tasks such as creating, deleting, and modifying objects and compiling policy.
D. Performs database tasks such as creating, deleting, and modifying objects and compiling as well as policy code generation.

Answer: C

NEW QUESTION 78
- (Exam Topic 1)
If you needed the Multicast MAC address of a cluster, what command would you run?

A. cphaprob –a if
B. cphaconf ccp multicast
C. cphaconf debug data
D. cphaprob igmp

Answer: D

NEW QUESTION 79
- (Exam Topic 1)
Identify the API that is not supported by Check Point currently.

A. R81 Management API
B. Identity Awareness Web Services API
C. Open REST API
D. OPSEC SDK

Answer: C

NEW QUESTION 84

- (Exam Topic 1)
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 87
- (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 92
- (Exam Topic 1)
Which of the following authentication methods ARE NOT used for Mobile Access?

A. RADIUS server
B. Username and password (internal, LDAP)
C. SecurID
D. TACACS+

Answer: D

NEW QUESTION 97
- (Exam Topic 1)
Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using the "mgmt_cli" command
B. Typing API commands from a dialog box inside the SmartConsole GUI application
C. Typing API commands using Gaia's secure shell(clish)19+
D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 100
- (Exam Topic 1)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 101
- (Exam Topic 1)
In R81 spoofing is defined as a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins
D. Making packets appear as if they come from an authorized IP address.

Answer: D

Explanation:
IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

NEW QUESTION 106
- (Exam Topic 1)
What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

A. Source address, Destination address, Source port, Destination port, Protocol
B. Source MAC address, Destination MAC address, Source port, Destination port, Protocol
C. Source address, Destination address, Source port, Destination port

D. Source address, Destination address, Destination port, Protocol

Answer: A

NEW QUESTION 110
- (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 113
- (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 114
- (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 119
- (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 122
- (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 126
- (Exam Topic 2)
John is using Management HA. Which Smartcenter should be connected to for making changes?

A. secondary Smartcenter
B. active Smartenter
C. connect virtual IP of Smartcenter HA
D. primary Smartcenter

Answer: B

NEW QUESTION 131
- (Exam Topic 2)
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day

Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Answer: A

NEW QUESTION 134
- (Exam Topic 2)
Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

A. You can assign only one profile per gateway and a profile can be assigned to one rule Only.
B. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.
C. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.
D. You can assign only one profile per gateway and a profile can be assigned to one or more rules.

Answer: C

NEW QUESTION 138
- (Exam Topic 2)
As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?

A. SFWDIR/smartevent/conf
B. $RTDIR/smartevent/conf
C. $RTDIR/smartview/conf
D. $FWDIR/smartview/conf

Answer: C

NEW QUESTION 143
- (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 148
- (Exam Topic 2)
Which GUI client is supported in R81?

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

Answer: C

NEW QUESTION 150
- (Exam Topic 2)
You need to see which hotfixes are installed on your gateway, which command would you use?

A. cpinfo –h all
B. cpinfo –o hotfix
C. cpinfo –l hotfix
D. cpinfo –y all

Answer: D

NEW QUESTION 153
- (Exam Topic 2)
As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
B. Fill Layer4 VPN –SSL VPN that gives users network access to all mobile applications.
C. Full Layer3 VPN –IPSec VPN that gives users network access to all mobile applications.
D. You can make sure that documents are sent to the intended recipients only.

Answer: C

NEW QUESTION 158
- (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 163
- (Exam Topic 2)
What is the purpose of a SmartEvent Correlation Unit?

A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.
C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.

Answer: C

NEW QUESTION 168
- (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 170
- (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 174
- (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 175
- (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 176
- (Exam Topic 2)
What is the command to see cluster status in cli expert mode?

A. fw ctl stat
B. clusterXL stat

C. clusterXL status
D. cphaprob stat

Answer: D

NEW QUESTION 179
- (Exam Topic 2)
How often does Threat Emulation download packages by default?

A. Once a week
B. Once an hour
C. Twice per day
D. Once per day

Answer: D

NEW QUESTION 184
- (Exam Topic 2)
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with _____ will not apply.

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

Answer: B

NEW QUESTION 185
- (Exam Topic 2)
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

A. Threat Emulation
B. Mobile Access
C. Mail Transfer Agent
D. Threat Cloud

Answer: B

NEW QUESTION 189
- (Exam Topic 2)
Which encryption algorithm is the least secured?

A. AES-128
B. AES-256
C. DES
D. 3DES

Answer: C

NEW QUESTION 191
- (Exam Topic 2)
Which command shows the current connections distributed by CoreXL FW instances?

A. fw ctl multik stat
B. fw ctl affinity -l
C. fw ctl instances -v
D. fw ctl iflist

Answer: A

NEW QUESTION 195
- (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 196
- (Exam Topic 2)

How do Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VP
B. Capsule Workspace provides a Desktop with usable applications.
C. Capsule Workspace can provide access to any application.
D. Capsule Connect provides Business data isolation.
E. Capsule Connect does not require an installed application at client.

Answer: A

NEW QUESTION 201
- (Exam Topic 2)
Please choose correct command to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90
B. mgmt: add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90
D. mgmt: add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 206
- (Exam Topic 2)
Which Check Point daemon monitors the other daemons?

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

Answer: C

NEW QUESTION 210
- (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 214
- (Exam Topic 2)
Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 216
- (Exam Topic 2)
The Correlation Unit performs all but the following actions:

A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
B. Generates an event based on the Event policy.
C. Assigns a severity level to the event.
D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.

Answer: C

NEW QUESTION 218
- (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 219
- (Exam Topic 2)
VPN Link Selection will perform the following when the primary VPN link goes down?

A. The Firewall will drop the packets.
B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
C. The Firewall will send out the packet on all interfaces.
D. The Firewall will inform the client that the tunnel is down.

Answer: B

NEW QUESTION 224
- (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 225
- (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 226
- (Exam Topic 2)
When gathering information about a gateway using CPINFO, what information is included or excluded when using the “-x” parameter?

A. Includes the registry
B. Gets information about the specified Virtual System
C. Does not resolve network addresses
D. Output excludes connection table

Answer: B

NEW QUESTION 227
- (Exam Topic 2)
Which one of the following is true about Threat Extraction?

A. Always delivers a file to user
B. Works on all MS Office, Executables, and PDF files
C. Can take up to 3 minutes to complete
D. Delivers file only if no threats found

Answer: A

NEW QUESTION 229
- (Exam Topic 2)
With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

A. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
B. For end users to access the native applications, they need to install the SSL Network Extender.
C. HTTPS for web-based applications and AES or RSA algorithm for native application
D. For end users to access the native application, they need to install the SSL Network Extender.
E. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
F. For end users to access the native applications, no additional software is required.
G. HTTPS for web-based applications and AES or RSA algorithm for native application
H. For end users to access the native application, no additional software is required.

Answer: A

NEW QUESTION 233
- (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 236
- (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 238
- (Exam Topic 2)
What is the most recommended way to install patches and hotfixes?

A. CPUSE Check Point Update Service Engine
B. rpm -Uv
C. Software Update Service
D. UnixinstallScript

Answer: A

NEW QUESTION 239
- (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 243
- (Exam Topic 2)
Which statement is true about ClusterXL?

A. Supports Dynamic Routing (Unicast and Multicast)
B. Supports Dynamic Routing (Unicast Only)
C. Supports Dynamic Routing (Multicast Only)
D. Does not support Dynamic Routing

Answer: A

NEW QUESTION 247
- (Exam Topic 2)
Customer’s R81 management server needs to be upgraded to R81.10. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R81 configuration, clean install R81.10 and import the configuration
B. CPUSE offline upgrade
C. CPUSE online upgrade
D. SmartUpdate upgrade

Answer: C

NEW QUESTION 251
- (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 252
- (Exam Topic 2)
John detected high load on sync interface. Which is most recommended solution?

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

Answer: A

NEW QUESTION 255
- (Exam Topic 2)
Which of the following links will take you to the SmartView web application?

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

Answer: B

NEW QUESTION 260
- (Exam Topic 2)
SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

A. 19090,22
B. 19190,22
C. 18190,80
D. 19009,443

Answer: D

NEW QUESTION 264
- (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 267
- (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 269
- (Exam Topic 2)
What is the benefit of “tw monitor” over “tcpdump”?

A. “fw monitor” reveals Layer 2 information, while “tcpdump” acts at Layer 3.
B. “fw monitor” is also available for 64-Bit operating systems.
C. With “fw monitor”, you can see the inspection points, which cannot be seen in “tcpdump”
D. “fw monitor” can be used from the CLI of the Management Server to collect information from multiple gateways.

Answer: C

NEW QUESTION 271
- (Exam Topic 2)
To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

A. fw ctl Dyn_Dispatch on
B. fw ctl Dyn_Dispatch enable
C. fw ctl multik set_mode 4
D. fw ctl multik set_mode 1

Answer: C

NEW QUESTION 275
- (Exam Topic 2)
SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

A. Analyzes each log entry as it arrives at the log server according to the Event Polic
B. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.
C. Correlates all the identified threats with the consolidation policy.
D. Collects syslog data from third party devices and saves them to the database.
E. Connects with the SmartEvent Client when generating threat reports.

Answer: A

NEW QUESTION 279
- (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 284
- (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 288
- (Exam Topic 2)
What is the port used for SmartConsole to connect to the Security Management Server?

A. CPMI port 18191/TCP
B. CPM port/TCP port 19009
C. SIC port 18191/TCP
D. https port 4434/TCP

Answer: A

NEW QUESTION 290
- (Exam Topic 2)
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

A. cphaprob set int fwha_vmac_global_param_enabled 1
B. clusterXL set int fwha_vmac_global_param_enabled 1
C. fw ctl set int fwha_vmac_global_param_enabled 1
D. cphaconf set int fwha_vmac_global_param_enabled 1

Answer: C

NEW QUESTION 295
- (Exam Topic 2)
SandBlast appliances can be deployed in the following modes:

A. using a SPAN port to receive a copy of the traffic only
B. detect only
C. inline/prevent or detect
D. as a Mail Transfer Agent and as part of the traffic flow only

Answer: C

NEW QUESTION 299
- (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 300
- (Exam Topic 3)
On what port does the CPM process run?

A. TCP 857
B. TCP 18192
C. TCP 900
D. TCP 19009

Answer: D

NEW QUESTION 302
- (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 307
- (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 309
- (Exam Topic 3)
The essential means by which state synchronization works to provide failover in the event an active member goes down, _____ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

A. ccp
B. cphaconf
C. cphad
D. cphastart

Answer: A

NEW QUESTION 314
- (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 319

- (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 321
- (Exam Topic 3)
To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int vmac global param enabled; result of command should return value 1
C. cphaprob-a if
D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: D

NEW QUESTION 322
- (Exam Topic 3)
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

A. Accounting
B. Suppression
C. Accounting/Suppression
D. Accounting/Extended

Answer: C

NEW QUESTION 325
- (Exam Topic 3)
Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?

A. /opt/CPshrd-R81/conf/local.arp
B. /var/opt/CPshrd-R81/conf/local.arp
C. $CPDIR/conf/local.arp
D. $FWDIR/conf/local.arp

Answer: D

NEW QUESTION 328
- (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 333
- (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 337
- (Exam Topic 3)
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all the following except:

A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution

Answer: A

Explanation:
Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:
• Use an automated script to perform common tasks
• Integrate Check Point products with 3rd party solutions
• Create products that use and enhance the Check Point solution References:

NEW QUESTION 342
- (Exam Topic 3)
Capsule Connect and Capsule Workspace both offer secured connection for remote users who are using their mobile devices. However, there are differences between the two.
Which of the following statements correctly identify each product's capabilities?

A. Workspace supports ios operating system, Android, and WP8, whereas Connect supports ios operating system and Android only
B. For compliance/host checking, Workspace offers the MDM cooperative enforcement, whereas Connect offers both jailbreak/root detection and MDM cooperative enforcement.
C. For credential protection, Connect uses One-time Password login support and has no SSO support, whereas Workspace offers both One-Time Password and certain SSO login support.
D. Workspace can support any application, whereas Connect has a limited number of application types which it will support.

Answer: C

NEW QUESTION 344
- (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 348
- (Exam Topic 3)
In which formats can Threat Emulation forensics reports be viewed in?

A. TXT, XML and CSV
B. PDF and TXT
C. PDF, HTML, and XML
D. PDF and HTML

Answer: C

NEW QUESTION 351
- (Exam Topic 3)
Office mode means that:

A. SecurID client assigns a routable MAC addres
B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
C. Users authenticate with an Internet browser and use secure HTTPS connection.
D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
E. Allows a security gateway to assign a remote client an IP addres
F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

NEW QUESTION 356
- (Exam Topic 3)
What command lists all interfaces using Multi-Queue?

A. cpmq get
B. show interface all
C. cpmq set
D. show multiqueue all

Answer: A

NEW QUESTION 357
- (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 361
- (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 366
- (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 371
- (Exam Topic 3)
Which NAT rules are prioritized first?

A. Post-Automatic/Manual NAT rules
B. Manual/Pre-Automatic NAT
C. Automatic Hide NAT
D. Automatic Static NAT

Answer: B

NEW QUESTION 373
- (Exam Topic 3)
What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

A. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
B. Security Gateway failover as well as Security Management Server failover is a manual procedure.
C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
D. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

Answer: A

NEW QUESTION 376
- (Exam Topic 3)
Which application should you use to install a contract file?

A. SmartView Monitor
B. WebUI
C. SmartUpdate
D. SmartProvisioning

Answer: C

NEW QUESTION 377
- (Exam Topic 3)
Which of the following commands shows the status of processes?

A. cpwd_admin -l
B. cpwd -l
C. cpwd admin_list
D. cpwd_admin list

Answer: D

NEW QUESTION 382

- (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 386
- (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 388
- (Exam Topic 3)
In the Firewall chain mode FFF refers to:

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

Answer: C

NEW QUESTION 393
- (Exam Topic 3)
In what way are SSL VPN and IPSec VPN different?

A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
C. IPSec VPN does not support two factor authentication, SSL VPN does support this
D. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.

Answer: D

NEW QUESTION 394
- (Exam Topic 3)
Which is not a blade option when configuring SmartEvent?

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

Answer: B

Explanation:
On the Management tab, enable these Software Blades: References:

NEW QUESTION 395
- (Exam Topic 3)
Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment.
Which details she need to fill in System Restore window before she can click OK button and test the backup?

A. Server, SCP, Username, Password, Path, Comment, Member
B. Server, TFTP, Username, Password, Path, Comment, All Members
C. Server, Protocol, Username, Password, Path, Comment, All Members
D. Server, Protocol, username Password, Path, Comment, Member

Answer: C

NEW QUESTION 400
- (Exam Topic 3)
The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated.
What is the most likely reason that the traffic is not accelerated?

A. There is a virus foun
B. Traffic is still allowed but not accelerated.
C. The connection required a Security server.
D. Acceleration is not enabled.
E. The traffic is originating from the gateway itself.

Answer: B

NEW QUESTION 403
- (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 404
- (Exam Topic 3)
Ken wants to obtain a configuration lock from other administrator on R81 Security Management Server. He can do this via WebUI or via CLI.
Which command should he use in CLI? (Choose the correct answer.)

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

Answer: D

NEW QUESTION 405
- (Exam Topic 3)
Which command would you use to set the network interfaces' affinity in Manual mode?

A. sim affinity -m
B. sim affinity -l
C. sim affinity -a
D. sim affinity -s

Answer: D

NEW QUESTION 407
- (Exam Topic 3)
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 411
- (Exam Topic 3)
When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

Answer: D

NEW QUESTION 414
- (Exam Topic 3)
For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

A. 20 minutes
B. 15 minutes
C. Admin account cannot be unlocked automatically
D. 30 minutes at least

Answer: D

NEW QUESTION 416
- (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 419
- (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

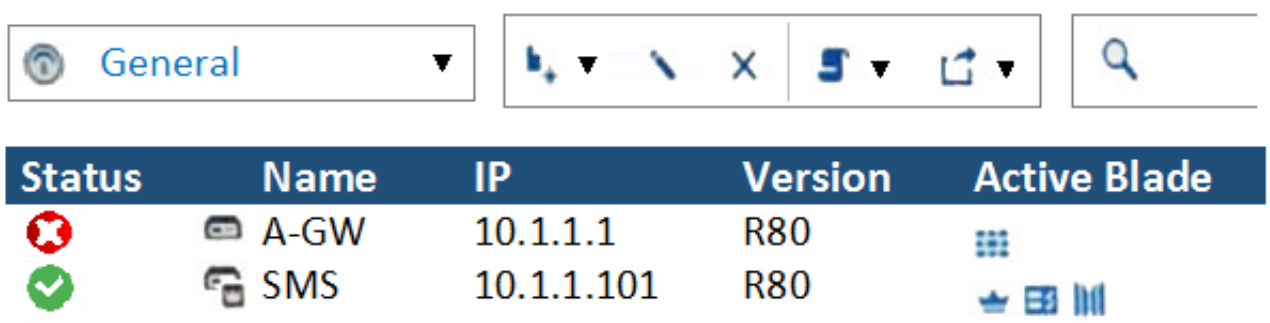
Explanation:
Virtual Router ID - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.

NEW QUESTION 420
- (Exam Topic 3)
You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

A. sim erdos –e 1
B. sim erdos – m 1
C. sim erdos –v 1
D. sim erdos –x 1

Answer: A

NEW QUESTION 422
- (Exam Topic 3)
What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)



A. SmartCenter Server cannot reach this Security Gateway.
B. There is a blade reporting a problem.
C. VPN software blade is reporting a malfunction.
D. Security Gateway’s MGNT NIC card is disconnected.

Answer: B

NEW QUESTION 427
- (Exam Topic 4)
Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

A. Auditor
B. Read Only All
C. Super User
D. Full Access

Answer: B

NEW QUESTION 431
- (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 432
- (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 435
- (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 436
- (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 441
- (Exam Topic 4)
Which Check Point daemon invokes and monitors critical processes and attempts to restart them if they fail?

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

Answer: C

NEW QUESTION 445
- (Exam Topic 4)
Which components allow you to reset a VPN tunnel?

A. vpn tu command or SmartView monitor
B. delete vpn ike sa or vpn she11 command
C. vpn tunnelutil or delete vpn ike sa command
D. SmartView monitor only

Answer: D

NEW QUESTION 447
- (Exam Topic 4)
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

A. Formal; corporate
B. Local; formal
C. Local; central
D. Central; local

Answer: D

NEW QUESTION 450
- (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 455
- (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 457
- (Exam Topic 4)
What are the services used for Cluster Synchronization?

A. 256H-CP tor Full Sync and 8116/UDP for Delta Sync
B. 8116/UDP for Full Sync and Delta Sync
C. TCP/256 for Full Sync and Delta Sync
D. No service needed when using Broadcast Mode

Answer: C

NEW QUESTION 461
- (Exam Topic 4)
Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances Steve's manager. Diana asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?

A. fw tab -t connections -s
B. fw tab -t connections
C. fw tab -t connections -c
D. fw tab -t connections -f

Answer: B

NEW QUESTION 466
- (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 468
- (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 471
- (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 475
- (Exam Topic 4)
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

A. All Connections (Clear or Encrypted)
B. Accept all encrypted traffic
C. Specific VPN Communities
D. All Site-to-Site VPN Communities

Answer: B

NEW QUESTION 477
- (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 480
- (Exam Topic 4)
Fill in the blank: A _____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

A. Clientless remote access
B. Clientless direct access
C. Client-based remote access
D. Direct access

Answer: A

NEW QUESTION 483
- (Exam Topic 4)
After having saved the Cllsh 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 usef account (e.
B. /home/admirV)
C. You can locate the file via SmartConsole > Command Line.
D. You have to launch the WebUl and go to "Config" -> "Export Conflg File" and specifly the destination directory of your local tile system
E. You cannot locate the file in the file system sine© Clish does not have any access to the bash fie system

Answer: B

NEW QUESTION 487
- (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 491
- (Exam Topic 4)
Choose the correct syntax to add a new host named “emailserver1” with IP address 10.50.23.90 using GAiA Management CLI?

A. mgmt_cli add host name “myHost12 ip” address 10.50.23.90
B. mgmt_cli add host name ip-address 10.50.23.90
C. mgmt_cli add host “emailserver1” address 10.50.23.90
D. mgmt_cli add host name “emailserver1” ip-address 10.50.23.90

Answer: D

Explanation:
Reference: https://weekly-geekly.github.io/articles/339924/index.html

NEW QUESTION 496
- (Exam Topic 4)
Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

A. cphaprob-aif
B. cp hap rob state
C. cphaprob list
D. probcpha -a if

Answer: A

NEW QUESTION 500
- (Exam Topic 4)
Which Queue in the Priority Queue has the maximum priority?

A. High Priority
B. Control
C. Routing
D. Heavy Data Queue

Answer: C

NEW QUESTION 501
- (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 503
- (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 507
- (Exam Topic 4)
Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Port
B. TCP Acknowledgment Number
C. Source Address
D. Destination Address

Answer: B

NEW QUESTION 512
- (Exam Topic 4)
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck
B. Active Directory Query
C. Account Unit Query
D. User Directory Query

Answer: B

Explanation:
Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION 513
- (Exam Topic 4)
Fill in the blank: An identity server uses a _____ for user authentication.

A. Shared secret
B. Certificate
C. One-time password

D. Token

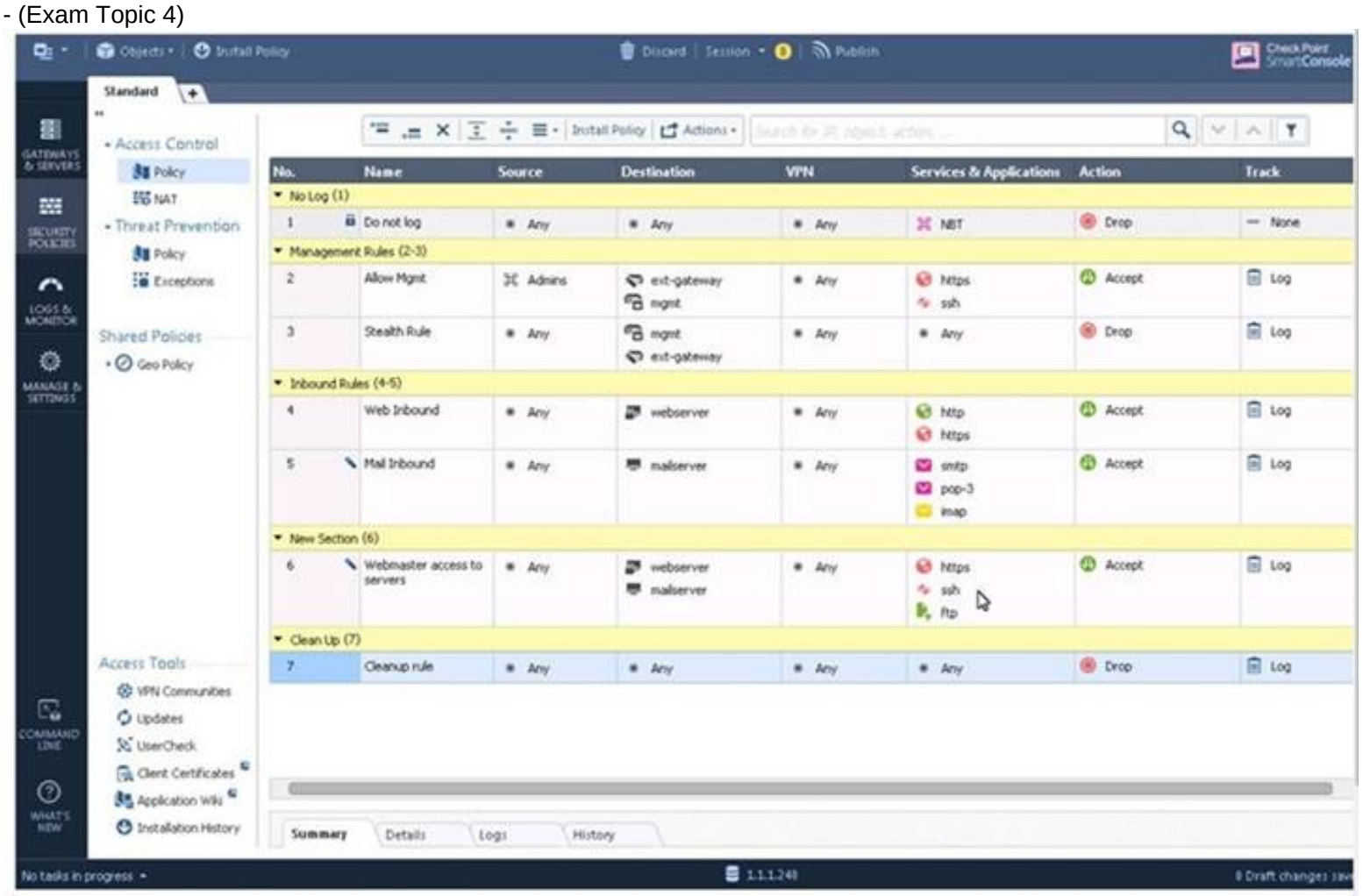
Answer: A

NEW QUESTION 516
- (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 517
- (Exam Topic 4)



What can we infer about the recent changes made to the Rule Base?

A. Rule 7 was created by the ‘admin’ administrator in the current session
B. 8 changes have been made by administrators since the last policy installation
C. The rules 1, 5 and 6 cannot be edited by the ‘admin’ administrator
D. Rule 1 and object webserver are locked by another administrator

Answer: D

NEW QUESTION 521
- (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 526
- (Exam Topic 4)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 528

- (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 529
- (Exam Topic 4)
On R81.10 the IPS Blade is managed by:

A. Threat Protection policy
B. Anti-Bot Blade
C. Threat Prevention policy
D. Layers on Firewall policy

Answer: C

NEW QUESTION 532
- (Exam Topic 4)
Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 536
- (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 539
- (Exam Topic 4)
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

A. Accept; redirect
B. Accept; drop
C. Redirect; drop
D. Drop; accept

Answer: D

NEW QUESTION 540
- (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 543
- (Exam Topic 4)
What is the best sync method in the ClusterXL deployment?

A. Use 1 cluster + 1st sync
B. Use 1 dedicated sync interface
C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
D. Use 2 clusters +1st sync + 2nd sync

Answer: B

NEW QUESTION 544
- (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 546
- (Exam Topic 4)
Which of the following is NOT supported by CPUSE?

A. Automatic download of full installation and upgrade packages
B. Automatic download of hotfixes
C. Installation of private hotfixes
D. Offline installations

Answer: D

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

NEW QUESTION 551
- (Exam Topic 4)
In the R81 SmartConsole, on which tab are Permissions and Administrators defined?

A. Security Policies
B. Logs and Monitor
C. Manage and Settings
D. Gateways and Servers

Answer: C

NEW QUESTION 552
- (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. After upgrading the hardware, increase the number of kernel instances using cpconfig
B. Hyperthreading must be enabled in the bios to use CoreXL
C. Run cprestart from dish
D. Administrator does not need to perform any tas
E. Check Point will make use of the newly installed CPU and Cores.

Answer: A

Explanation:
https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG R81
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/ cpconfig -> Enter the number of the Check Point CoreXL option. (Enter 1 to select Change the number of firewall instances. OR Enter 2 for the option Change the number of IPv6 firewall instances.) -> Enter the total number of IPv4 (IPv6) CoreXL Firewall instances you wish the Security Gateway to run. Follow the instructions on the screen. -> Exit from the cpconfig menu.
- Reboot the Security Gateway.

NEW QUESTION 557
- (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 559
- (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 561
- (Exam Topic 4)
Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

A. assign privileges to users.
B. edit the home directory of the user.
C. add users to your Gaia system.
D. assign user rights to their home directory in the Security Management Server.

Answer: D

NEW QUESTION 562
- (Exam Topic 4)
Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

A. cpm
B. fwd
C. cpd
D. fwmD18912E1457D5D1DDCBD40AB3BF70D5D

Answer: D

NEW QUESTION 567
- (Exam Topic 4)
Which command is used to obtain the configuration lock in Gaia?

A. Lock database override
B. Unlock database override
C. Unlock database lock
D. Lock database user

Answer: A

Explanation:
Obtaining a Configuration Lock

NEW QUESTION 568
- (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 569
- (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 573
- (Exam Topic 4)

Which 3 types of tracking are available for Threat Prevention Policy?

A. SMS Alert, Log, SNMP alert
B. Syslog, None, User-defined scripts
C. None, Log, Syslog
D. Alert, SNMP trap, Mail

Answer: B

NEW QUESTION 575
- (Exam Topic 4)
Packet acceleration (SecureXL) identifies connections by several attributes- Which of the attributes is NOT used for identifying connection?

A. Source Address
B. Destination Address
C. TCP Acknowledgment Number
D. Source Port

Answer: C

Explanation:
https //sc1.checkpoint.com/documents/R77/CP R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 578
- (Exam Topic 4)
What is false regarding a Management HA environment?

A. Only one Management Server should be active, while any others be in standby mode
B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.
C. SmartConsole can connect to any management server in Readonly mode.
D. Synchronization will occur automatically with each Publish event if the Standby servers are available.

Answer: B

NEW QUESTION 580
- (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 582
- (Exam Topic 4)
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

A. Toni? AND 10.0.4.210 NOT 10.0.4.76
B. To** AND 10.0.4.210 NOT 10.0.4.76
C. Ton* AND 10.0.4.210 NOT 10.0.4.75
D. "Toni" AND 10.0.4.210 NOT 10.0.4.76

Answer: D

NEW QUESTION 584
- (Exam Topic 4)
The Check Point history feature in R81 provides the following:

A. View install changes and install specific version
B. View install changes
C. Policy Installation Date, view install changes and install specific version
D. Policy Installation Date only

Answer: D

NEW QUESTION 585
- (Exam Topic 4)
Which options are given on features, when editing a Role on Gaia Platform?

A. Read/Write, Read Only
B. Read/Write, Read Only, None
C. Read/Write, None
D. Read Only, None

Answer: B

NEW QUESTION 588
- (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 590
- (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 normally
C. All connections that were initiated before the upgrade will be handled by the standby gateway
D. All connections that were initiated before the upgrade will be handled by the active gateway

Answer: A

NEW QUESTION 595
- (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 598
- (Exam Topic 4)
In Advanced Permanent Tunnel Configuration, to set the amount of time the tunnel test runs without a response before the peer host is declared ‘down’, you would set the ?

A. life sign polling interval
B. life sign timeout
C. life_sign_polling_interval
D. life_sign_timeout

Answer: D

Explanation:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm? topic=documents/R77/CP_R77_VPN_AdminGuide/14018

NEW QUESTION 601
- (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 604
- (Exam Topic 4)
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 609
- (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 610
- (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 615
- (Exam Topic 4)
Which software blade does NOT accompany the Threat Prevention policy?

A. Anti-virus
B. IPS
C. Threat Emulation
D. Application Control and URL Filtering

Answer: D

NEW QUESTION 617
- (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 621
- (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

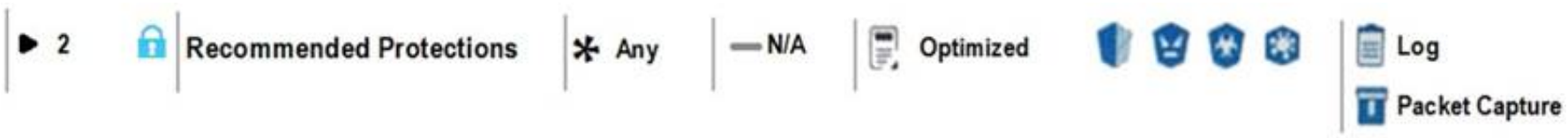
NEW QUESTION 623
- (Exam Topic 4)
Which of the following is a task of the CPD process?

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 628
- (Exam Topic 4)
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



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 632
- (Exam Topic 4)
You want to allow your Mobile Access Users to connect to an internal file share. Adding the Mobile Application 'File Share' to your Access Control Policy in the SmartConsole didn't work. You will be only allowed to select Services for the 'Service & Application' column How to fix it?

A. A Quantum Spark Appliance is selected as Installation Target for the policy packet.
B. The Mobile Access Blade is not enabled for the Access Control Layer of the policy.
C. The Mobile Access Policy Source under Gateway properties Is set to Legacy Policy and not to Unified Access Policy.
D. The Mobile Access Blade is not enabled under Gateway properties.

Answer: C

NEW QUESTION 637
- (Exam Topic 4)
What state is the Management HA in when both members have different policies/databases?

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

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/
html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/98838

NEW QUESTION 640
- (Exam Topic 4)
What is false regarding prerequisites for the Central Deployment usage?

A. The administrator must have write permission on SmartUpdate
B. Security Gateway must have the latest CPUSE Deployment Agent
C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.
D. The Security Gateway must have a policy installed

Answer: D

NEW QUESTION 644
- (Exam Topic 4)
You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

A. Logging has disk space issue
B. Change logging storage options on the logging server or Security Management Server properties and install database.
C. Data Awareness is not enabled.
D. Identity Awareness is not enabled.
E. Logs are arriving from Pre-R81 gateways.

Answer: A

NEW QUESTION 645
- (Exam Topic 4)
An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?

A. Slow Path
B. Fast Path
C. Medium Path
D. Accelerated Path

Answer: D

NEW QUESTION 648
- (Exam Topic 4)
What is the command to check the status of Check Point processes?

A. top
B. cptop
C. cphaprob list
D. cpwd_admin list

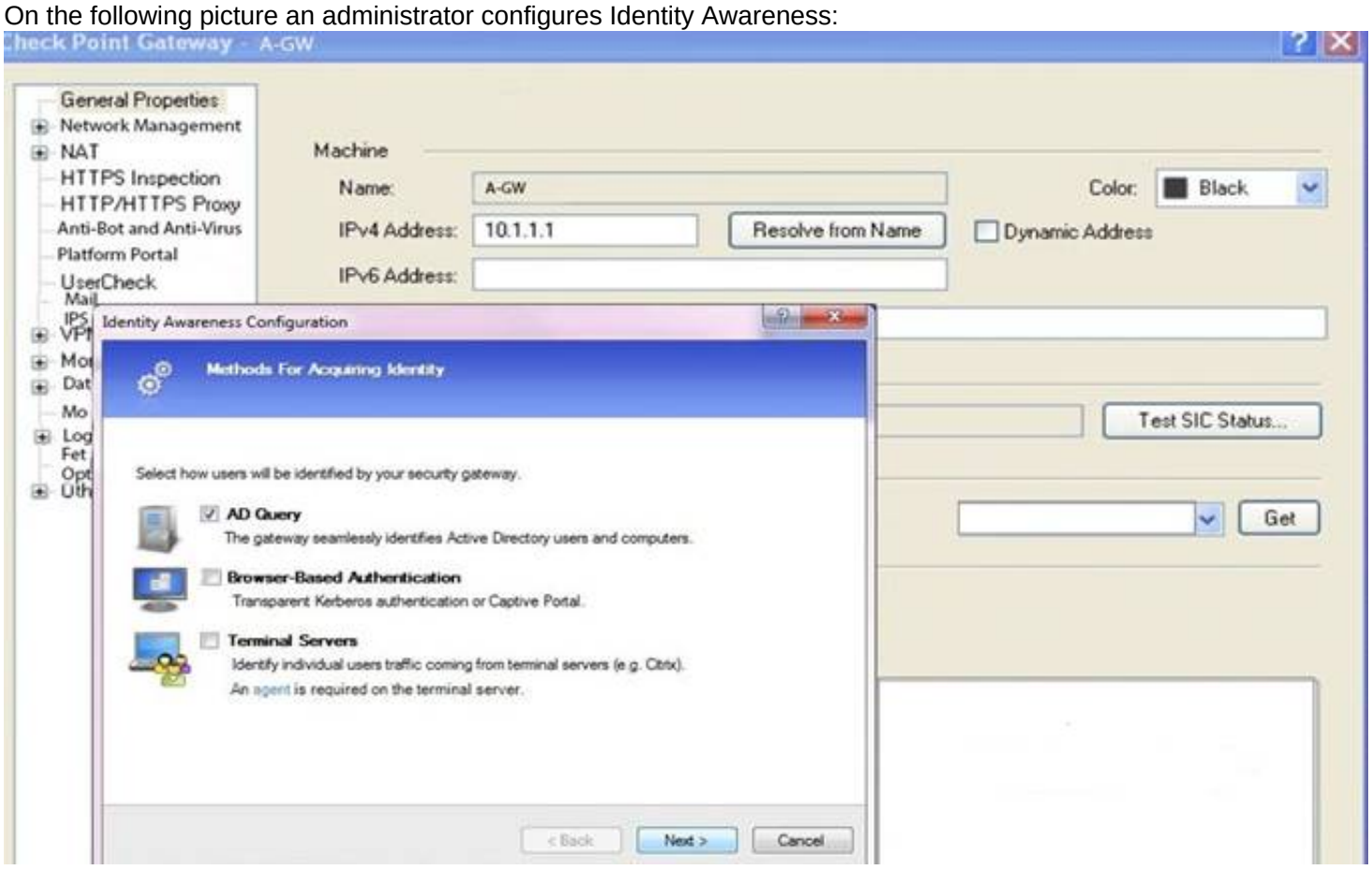
Answer: D

NEW QUESTION 653
- (Exam Topic 4)
UserCheck objects in the Application Control and URL Filtering rules allow the gateway to communicate with the users. Which action is not supported in UserCheck objects?

A. Ask
B. Drop
C. Inform
D. Reject

Answer: D

NEW QUESTION 657
- (Exam Topic 4)
On the following picture an administrator configures Identity Awareness:



After clicking “Next” the above configuration is supported by:

A. Kerberos SSO which will be working for Active Directory integration
B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.
C. Obligatory usage of Captive Portal.
D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Answer: B

NEW QUESTION 662
- (Exam Topic 4)
What is the recommended way to have a redundant Sync connection between the cluster nodes?

A. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per nod
B. Connect both Sync interfaces without using a switch.
C. Use a group of bonded interface
D. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define a Virtual IP for the Sync interface.
E. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per nod
F. Use two different Switches to connect both Sync interfaces.
G. Use a group of bonded interfaces connected to different switche
H. Define a dedicated sync interface, only one interface per node using the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management.

Answer: C

NEW QUESTION 667
- (Exam Topic 4)
What does Backward Compatibility mean upgrading the Management Server and how can you check it?

A. The Management Server is able to manage older Gateway
B. The lowest supported version is documented in the Installation and Upgrade Guide
C. The Management Server is able to manage older Gateways The lowest supported version is documented in the Release Notes
D. You will be able to connect to older Management Server with the SmartConsol
E. The lowest supported version is documented in the Installation and Upgrade Guide
F. You will be able to connect to older Management Server with the SmartConsole The lowest supported version is documented in the Release Notes

Answer: A

NEW QUESTION 671
- (Exam Topic 4)
Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (EL-A) services.

A. DASSERVICE
B. FWD
C. CPVIEWD
D. CPD

Answer: A

NEW QUESTION 675
- (Exam Topic 4)
SmartConsole R81 x requires the following ports to be open for SmartEvent.

A. 19009, 19090 & 443
B. 19009, 19004 & 18190
C. 18190 & 443
D. 19009, 18190 & 443

Answer: D

NEW QUESTION 678
- (Exam Topic 4)
At what point is the Internal Certificate Authority (ICA) created?

A. Upon creation of a certificate.
B. During the primary Security Management Server installation process.
C. When an administrator decides to create one.
D. When an administrator initially logs into SmartConsole.

Answer: B

NEW QUESTION 682
- (Exam Topic 4)
After verifying that API Server is not running, how can you start the API Server?

A. Run command "set api start" in CLISH mode
B. Run command "mgmt cli set api start" in Expert mode
C. Run command "mgmt api start" in CLISH mode
D. Run command "api start" in Expert mode

Answer: B

NEW QUESTION 686
- (Exam Topic 4)
When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Answer: C

NEW QUESTION 690
- (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 695
- (Exam Topic 4)
Which command is used to add users to or from existing roles?

A. Add rba user <User Name> roles <List>
B. Add rba user <User Name>
C. Add user <User Name> roles <List>
D. Add user <User Name>

Answer: A

NEW QUESTION 698
- (Exam Topic 4)
What is "Accelerated Policy Installation"?

A. Starting R81, the Desktop Security Policy installation process is accelerated thereby reducing the duration of the process significantly
B. Starting R81, the QoS Policy installation process is accelerated thereby reducing the duration of the process significantly
C. Starting R81, the Access Control Policy installation process is accelerated thereby reducing the duration of the process significantly
D. Starting R81, the Threat Prevention Policy installation process is accelerated thereby reducing the duration of the process significantly

Answer: C

NEW QUESTION 703
- (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 707
- (Exam Topic 4)
What are the two modes for SNX (SSL Network Extender)?

A. Network Mode and Application Mode
B. Visitor Mode and Office Mode
C. Network Mode and Hub Mode
D. Office Mode and Hub Mode

Answer: A

NEW QUESTION 708
- (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 713
- (Exam Topic 4)
SmartEvent uses it's event policy to identify events. How can this be customized?

A. By modifying the firewall rulebase
B. By creating event candidates

C. By matching logs against exclusions
D. By matching logs against event rules

Answer: D

NEW QUESTION 714
- (Exam Topic 4)
How many interfaces can you configure to use the Multi-Queue feature?

A. 10 interfaces
B. 3 interfaces
C. 4 interfaces
D. 5 interfaces

Answer: D

NEW QUESTION 716
- (Exam Topic 4)
What are not possible commands to acquire the lock in order to make changes in Clish or Web GUI?

A. set config-lock on override
B. Click the Lock icon in the WebUI
C. "set rbac rw = 1"
D. lock database override

Answer: C

NEW QUESTION 719
- (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 720
- (Exam Topic 4)
The “MAC magic” value must be modified under the following condition:

A. There is more than one cluster connected to the same VLAN
B. A firewall cluster is configured to use Multicast for CCP traffic
C. There are more than two members in a firewall cluster
D. A firewall cluster is configured to use Broadcast for CCP traffic

Answer: D

NEW QUESTION 725
- (Exam Topic 4)
Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up.
B. There is Load Sharing solution set up.
C. Only when there is Unicast solution set up.
D. There is High Availability solution set up.

Answer: D

NEW QUESTION 727
- (Exam Topic 4)
Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .

A. Firewall policy install
B. Threat Prevention policy install
C. Anti-bot policy install
D. Access Control policy install

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81/CP_R81BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 730

- (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 735
- (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 740
- (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 742
- (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 746
- (Exam Topic 4)
What are the three SecureXL Templates available in R81.10?

A. PEP Template
B. QoS Template
C. VPN Templates
D. Accept Template
E. Drop Template
F. NAT Templates
G. Accept Template
H. Drop Template
I. Reject Templates
J. Accept Template
K. PDP Template
L. PEP Templates

Answer: B

NEW QUESTION 747
- (Exam Topic 4)
Which one of the following is NOT a configurable Compliance Regulation?

A. GLBA
B. CJIS
C. SOCI
D. NCIPA

Answer: C

NEW QUESTION 749
- (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 754
.....

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