Exam Questions 156-315.81

Check Point Certified Security Expert R81

https://www.2passeasy.com/dumps/156-315.81/

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)
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 4
- (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 5
- (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 6
- (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 7
- (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 8
- (Exam Topic 1)
You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

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

Answer: C

NEW QUESTION 9
- (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 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 tool _____ generates a R81 Security Gateway configuration report.

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

Answer: C

NEW QUESTION 11
- (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 16
- (Exam Topic 1)
Advanced Security Checkups can be easily conducted within:

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

Answer: A

NEW QUESTION 19
- (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 24
- (Exam Topic 1)
What happen when IPS profile is set in Detect Only Mode for troubleshooting?

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

Answer: C

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

NEW QUESTION 27
- (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 32
- (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 36
- (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 39
- (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 43
- (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 47
- (Exam Topic 1)
The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

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

Answer: A

NEW QUESTION 49
- (Exam Topic 1)
Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 52
- (Exam Topic 1)
To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:

A. fw ctl multik set_mode 1
B. fw ctl Dynamic_Priority_Queue on
C. fw ctl Dynamic_Priority_Queue enable
D. fw ctl multik set_mode 9

Answer: D

NEW QUESTION 53
- (Exam Topic 1)
Which command shows actual allowed connections in state table?

A. fw tab –t StateTable
B. fw tab –t connections
C. fw tab –t connection
D. fw tab connections

Answer: B

NEW QUESTION 56
- (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 61
- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 65
- (Exam Topic 1)
In R81, how do you manage your Mobile Access Policy?

A. Through the Unified Policy
B. Through the Mobile Console
C. From SmartDashboard
D. From the Dedicated Mobility Tab

Answer: A

NEW QUESTION 69
- (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 72
- (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 77
- (Exam Topic 1)
The Event List within the Event tab contains:

A. a list of options available for running a query.
B. the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
C. events generated by a query.
D. the details of a selected event.

Answer: C

NEW QUESTION 79
- (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 84
- (Exam Topic 1)
Which two of these Check Point Protocols are used by SmartEvent Processes?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

Answer: D

NEW QUESTION 88
- (Exam Topic 1)
R81.10 management server can manage gateways with which versions installed?

A. Versions R77 and higher
B. Versions R76 and higher
C. Versions R75.20 and higher
D. Versions R75 and higher

Answer: C

NEW QUESTION 91
- (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 92
- (Exam Topic 1)
What is the correct command to observe the Sync traffic in a VRRP environment?

A. fw monitor –e “accept[12:4,b]=224.0.0.18;”
B. fw monitor –e “accept port(6118;”
C. fw monitor –e “accept proto=mcVRRP;”
D. fw monitor –e “accept dst=224.0.0.18;”

Answer: D

NEW QUESTION 97
- (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 98
- (Exam Topic 1)
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

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

Answer: D

NEW QUESTION 103
- (Exam Topic 1)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 104
- (Exam Topic 1)
To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 107
- (Exam Topic 1)
CoreXL is supported when one of the following features is enabled:

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

Answer: B

Explanation:
CoreXL does not support Check Point Suite with these features: References:

NEW QUESTION 111
- (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 112
- (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 117
- (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 121
- (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 124
- (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 129

- (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 132
- (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 134
- (Exam Topic 2)
You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command. You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

A. cphaprob –f register
B. cphaprob –d –s report
C. cpstat –f all
D. cphaprob –a list

Answer: D

NEW QUESTION 138
- (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 143
- (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 144
- (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 145
- (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 146
- (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 151
- (Exam Topic 2)
Which configuration file contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status?

A. $FWDIR/database/fwauthd.conf
B. $FWDIR/conf/fwauth.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/state/fwauthd.conf

Answer: C

NEW QUESTION 154
- (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 156
- (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 160
- (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 165
- (Exam Topic 2)
Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 170
- (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 174
- (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 176
- (Exam Topic 2)
SmartEvent does NOT use which of the following procedures to identify events:

A. Matching a log against each event definition
B. Create an event candidate
C. Matching a log against local exclusions
D. Matching a log against global exclusions

Answer: C

Explanation:
Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:
• Matching a Log Against Global Exclusions
• Matching a Log Against Each Event Definition
• Creating an Event Candidate
• When a Candidate Becomes an Event References:

NEW QUESTION 177
- (Exam Topic 2)
From SecureXL perspective, what are the tree paths of traffic flow:

A. Initial Path; Medium Path; Accelerated Path
B. Layer Path; Blade Path; Rule Path
C. Firewall Path; Accept Path; Drop Path
D. Firewall Path; Accelerated Path; Medium Path

Answer: D

NEW QUESTION 182
- (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 186
- (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 189
- (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 192
- (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 193
- (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 195
- (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 196
- (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 201
- (Exam Topic 2)
Which command is used to display status information for various components?

A. show all systems
B. show system messages
C. sysmess all
D. show sysenv all

Answer: D

NEW QUESTION 204
- (Exam Topic 2)
What is the command to check the status of the SmartEvent Correlation Unit?

A. fw ctl get int cpsead_stat

B. cpstat cpsead
C. fw ctl stat cpsemd
D. cp_conf get_stat cpsemd

Answer: B

NEW QUESTION 206
- (Exam Topic 2)
Where do you create and modify the Mobile Access policy in R81?

A. SmartConsole
B. SmartMonitor
C. SmartEndpoint
D. SmartDashboard

Answer: A

NEW QUESTION 208
- (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 213
- (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 216
- (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 217
- (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 222
- (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 226
- (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 227
- (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 231
- (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 235
- (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 236
- (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 240
- (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 245
- (Exam Topic 2)
To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

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

Answer: B

NEW QUESTION 250
- (Exam Topic 3)
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

A. All UDP packets
B. All IPv6 Traffic
C. All packets that match a rule whose source or destination is the Outside Corporate Network
D. CIFS packets

Answer: D

NEW QUESTION 254
- (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 257
- (Exam Topic 3)
Joey wants to upgrade from R75.40 to R81 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this.
What is one of the requirements for his success?

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

NEW QUESTION 262
- (Exam Topic 3)
Which Check Point software blade provides Application Security and identity control?

A. Identity Awareness
B. Data Loss Prevention
C. URL Filtering
D. Application Control

Answer: D

NEW QUESTION 263
- (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 264
- (Exam Topic 3)
The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

A. Next Generation Threat Prevention
B. Next Generation Threat Emulation
C. Next Generation Threat Extraction
D. Next Generation Firewall

Answer: B

NEW QUESTION 269
- (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 273
- (Exam Topic 3)
You have a Gateway is running with 2 cores. You plan to add a second gateway to build a cluster and used a device with 4 cores.
How many cores can be used in a Cluster for Firewall-kernel on the new device?

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

Answer: D

NEW QUESTION 275
- (Exam Topic 3)
GAiA Software update packages can be imported and installed offline in situation where:

A. Security Gateway with GAiA does NOT have SFTP access to Internet
B. Security Gateway with GAiA does NOT have access to Internet.
C. Security Gateway with GAiA does NOT have SSH access to Internet.
D. The desired CPUSE package is ONLY available in the Check Point CLOUD.

Answer: B

NEW QUESTION 278
- (Exam Topic 3)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 279
- (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 283
- (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 284
- (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 288
- (Exam Topic 3)
What is the minimum amount of RAM needed for a Threat Prevention Appliance?

A. 6 GB
B. 8GB with Gaia in 64-bit mode
C. 4 GB
D. It depends on the number of software blades enabled

Answer: C

NEW QUESTION 289
- (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 294
- (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 298
- (Exam Topic 3)
Which of the following is NOT an option to calculate the traffic direction?

A. Incoming
B. Internal
C. External
D. Outgoing

Answer: D

NEW QUESTION 301
- (Exam Topic 3)
What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

A. S
B. W
C. C
D. Space bar

Answer: C

NEW QUESTION 306
- (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 310
- (Exam Topic 3)
Check Point security components are divided into the following components:

A. GUI Client, Security Gateway, WebUI Interface
B. GUI Client, Security Management, Security Gateway
C. Security Gateway, WebUI Interface, Consolidated Security Logs
D. Security Management, Security Gateway, Consolidate Security Logs

Answer: B

NEW QUESTION 313
- (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 315
- (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 318
- (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 322
- (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 324
- (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 328
- (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 333
- (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 338
- (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 340
- (Exam Topic 3)
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

A. User Directory
B. Captive Portal and Transparent Kerberos Authentication
C. Captive Portal
D. UserCheck

Answer: B

NEW QUESTION 345
- (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 348
- (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 352
- (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 354
- (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 359
- (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 360
- (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 364
- (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 368
- (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.

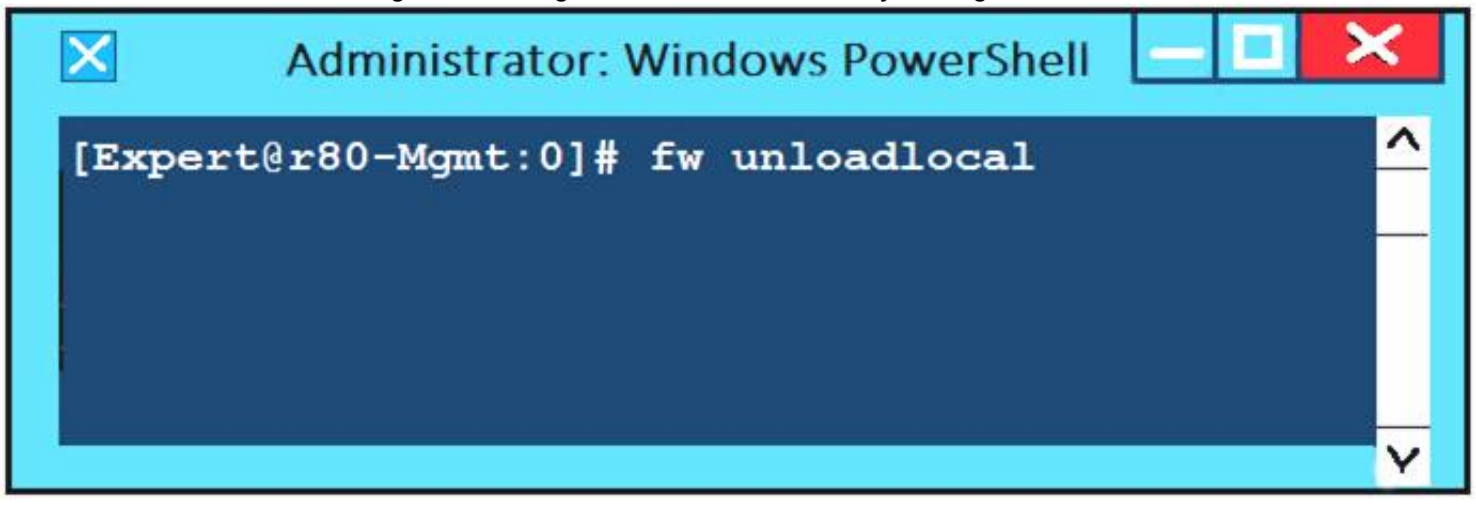
Answer: B

NEW QUESTION 371
- (Exam Topic 3)
With MTA (Mail Transfer Agent) enabled the gateways manages SMTP traffic and holds external email with potentially malicious attachments. What is required in order to enable MTA (Mail Transfer Agent) functionality in the Security Gateway?

A. Threat Cloud Intelligence
B. Threat Prevention Software Blade Package
C. Endpoint Total Protection
D. Traffic on port 25

Answer: B

NEW QUESTION 372
- (Exam Topic 3)
What will be the effect of running the following command on the Security Management Server?



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

Answer: A

NEW QUESTION 374
- (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 378
- (Exam Topic 3)
What is the responsibility of SOLR process on R81.10 management server?

A. Validating all data before it's written into the database
B. It generates indexes of data written to the database
C. Communication between SmartConsole applications and the Security Management Server
D. Writing all information into the database

Answer: B

NEW QUESTION 380
- (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 384
- (Exam Topic 3)
Which path below is available only when CoreXL is enabled?

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

Answer: C

NEW QUESTION 387
- (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 389
- (Exam Topic 3)
What must you do first if “fwm sic_reset” could not be completed?

A. Cpstop then find keyword “certificate” in objects_5_0.C and delete the section
B. Reinitialize SIC on the security gateway then run “fw unloadlocal”
C. Reset SIC from Smart Dashboard
D. Change internal CA via cpconfig

Answer: D

NEW QUESTION 394
- (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 397
- (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 402
- (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 405
- (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 407
- (Exam Topic 3)
With SecureXL enabled, accelerated packets will pass through the following:

A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
B. Network Interface Card, Check Point Firewall Kernal, and the Acceleration Device
C. Network Interface Card and the Acceleration Device
D. Network Interface Card, OSI Network Layer, and the Acceleration Device

Answer: C

NEW QUESTION 409
- (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

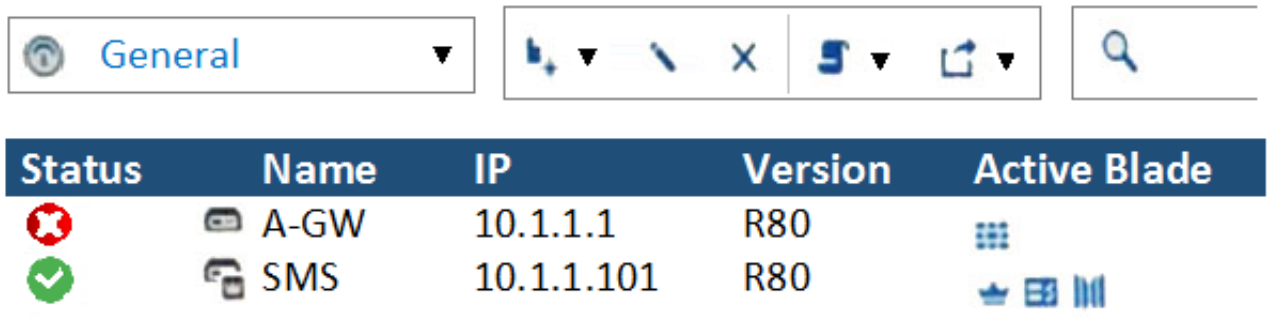
Answer: A

NEW QUESTION 411
- (Exam Topic 3)
When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related entries are present.
Which phase of the VPN negotiations has failed?

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

Answer: A

NEW QUESTION 415
- (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 416
- (Exam Topic 4)
Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command "cpconfig" to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances "Primary & Secondary" Which configuration option does she need to look for:

A. Certificate's Fingerprint
B. Random Pool
C. CA Authority
D. Certificate Authority

Answer: D

NEW QUESTION 417
- (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 419
- (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 420
- (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 423
- (Exam Topic 4)
There are multiple types of licenses for the various VPN components and types. License type related to management and functioning of Remote Access VPNs are - which of the following license requirement statement is NOT true:

A. MobileAccessLicense ° This license is required on the Security Gateway for the following Remote Access solutions
B. EndpointPolicyManagementLicense ° The Endpoint Security Suite includes blades other than the Remote Access VPN, hence this license is required to manage the suite
C. EndpointContainerLicense ° The Endpoint Software Blade Licenses does not require an Endpoint Container License as the base
D. IPSecVPNLicense • This license is installed on the VPN Gateway and is a basic requirement for a Remote Access VPN solution

Answer: C

NEW QUESTION 424
- (Exam Topic 4)
Which of the following is NOT a type of Endpoint Identity Agent?

A. Terminal
B. Light
C. Full
D. Custom

Answer: A

NEW QUESTION 427
- (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 429
- (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 434
- (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 435

- (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 440
- (Exam Topic 4)
When using the Mail Transfer Agent, where are the debug logs stored?

A. $FWDIR/bin/emaild.mt
B. elg
C. $FWDIR/log/mtad elg
D. /var/log/mail.mta elg
E. $CPDIR/log/emaild elg

Answer: C

NEW QUESTION 444
- (Exam Topic 4)
How does the Anti-Virus feature of the Threat Prevention policy block traffic from infected websites?

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

Answer: D

NEW QUESTION 449
- (Exam Topic 4)
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via
e-m ail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links.
Which component of SandBlast protection is her company using on a Gateway?

A. SandBlast Threat Emulation
B. SandBlast Agent
C. Check Point Protect
D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 452
- (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 454
- (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 458
- (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 460
- (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 461
- (Exam Topic 4)
What a valid SecureXL paths in R81.10?

A. F2F (Slow path). Templated Pat
B. PQX and F2V
C. F2F (Slow path). PXL, QXL and F2V
D. F2F (Slow path), Accelerated Path, PQX and F2V
E. F2F (Slow path), Accelerated Path, Medium Path and F2V

Answer: D

NEW QUESTION 463
- (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 464
- (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 466
- (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 467
- (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 472
- (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 476
- (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 481
- (Exam Topic 4)
What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

A. Mutually Trusted Certificate Authorities
B. Shared User Certificates
C. Shared Secret Passwords
D. Unique Passwords

Answer: A

NEW QUESTION 484
- (Exam Topic 4)
What traffic does the Anti-bot feature block?

A. Command and Control traffic from hosts that have been identified as infected
B. Command and Control traffic to servers with reputation for hosting malware
C. Network traffic that is directed to unknown or malicious servers
D. Network traffic to hosts that have been identified as infected

Answer: A

NEW QUESTION 488
- (Exam Topic 4)
GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

A. Check Point Update Service Engine
B. Check Point Software Update Agent
C. Check Point Remote Installation Daemon (CPRID)
D. Check Point Software Update Daemon

Answer: A

NEW QUESTION 492
- (Exam Topic 4)
Which command will reset the kernel debug options to default settings?

A. fw ctl dbg -a 0
B. fw ctl dbg resetall
C. fw ctl debug 0
D. fw ctl debug set 0

Answer: C

NEW QUESTION 495
- (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 498
- (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 499
- (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 504
- (Exam Topic 4)
What solution is Multi-queue intended to provide?

A. Improve the efficiency of traffic handling by SecureXL SNDs
B. Reduce the confusion for traffic capturing in FW Monitor
C. Improve the efficiency of CoreXL Kernel Instances
D. Reduce the performance of network interfaces

Answer: C

NEW QUESTION 506
- (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 510
- (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 514
- (Exam Topic 4)
Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when _____.

A. The license is attached to the wrong Security Gateway.
B. The existing license expires.
C. The license is upgraded.
D. The IP address of the Security Management or Security Gateway has changed.

Answer: A

NEW QUESTION 517
- (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 520
- (Exam Topic 4)
You need to change the MAC-address on eth2 interface of the gateway. What is the correct way to change MAC-address in Check Point Gaia?

A. In CLISH run: set interface eth2 mac-addr 11:11:11:11:11:11
B. In expert-mode run ifconfig eth1 hw 11:11:11:11 11 11
C. In CLISH run set interface eth2 hw-addr 11 11 11:11:11 11
D. In expert-mode run: ethtool -4 eth2 mac 11 11:11:11:11:11

Answer: A

NEW QUESTION 524
- (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 529
- (Exam Topic 4)
What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?

A. 1-254
B. 1-255
C. 0-254
D. 0 – 255

Answer: B

NEW QUESTION 530
- (Exam Topic 4)
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

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

Answer: B

NEW QUESTION 532

- (Exam Topic 4)
An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

A. IPsec VPN blade should be enabled on both Security Gateway.
B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 533
- (Exam Topic 4)
Alice works for a big security outsourcing provider company and as she receives a lot of change requests per day she wants to use for scripting daily (asks the API services from Check Point fof the Management API. Firstly she needs to be aware if the API services are running for the management. Which of the following Check Point Command is true:

A. api mgmt status
B. api status
C. status api
D. status mgmt apt

Answer: B

NEW QUESTION 534
- (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

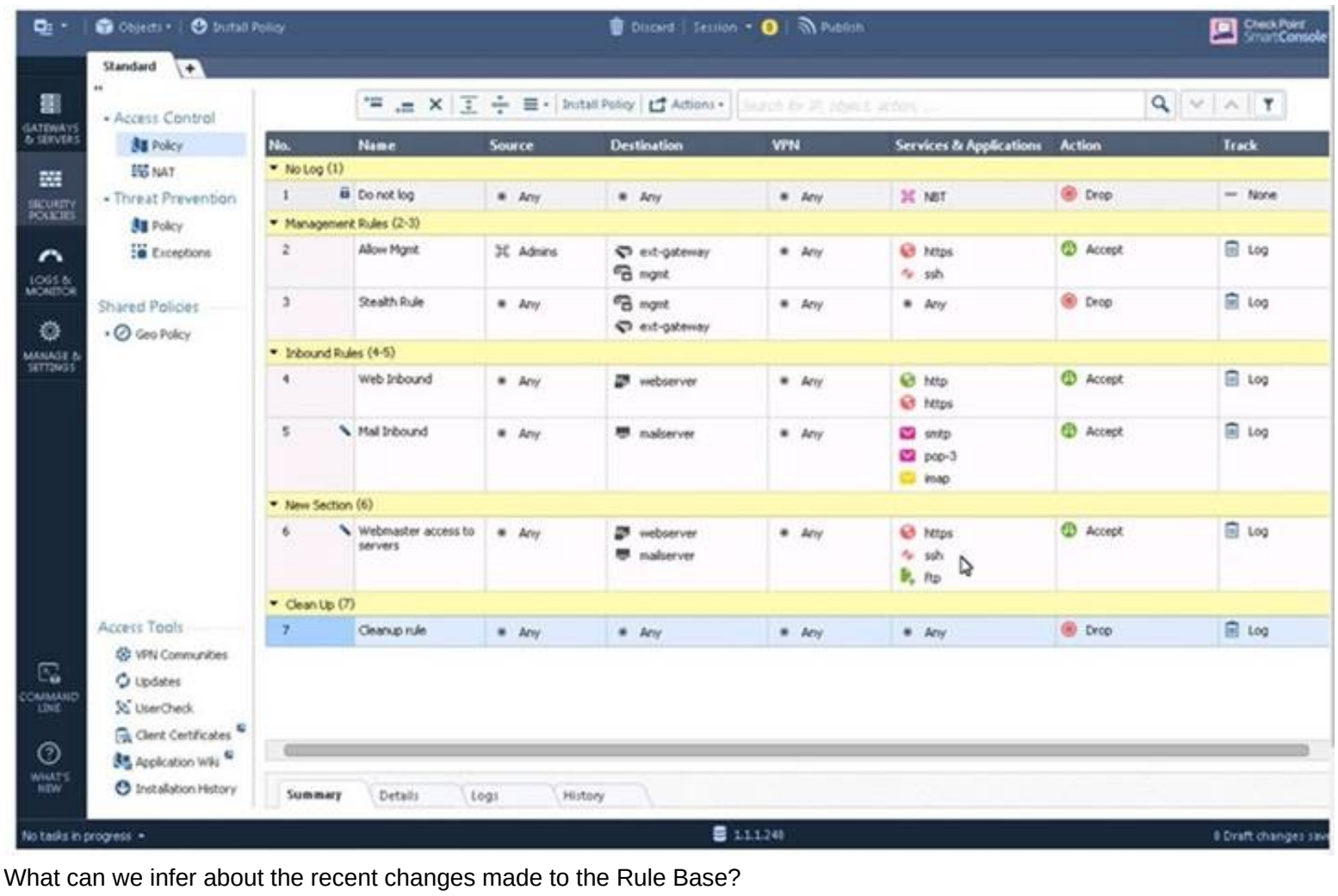
Answer: B

NEW QUESTION 535
- (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 536
- (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 537
- (Exam Topic 4)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 539
- (Exam Topic 4)
What is the base level encryption key used by Capsule Docs?

A. RSA 2048
B. RSA 1024
C. SHA-256
D. AES

Answer: A

NEW QUESTION 542
- (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 547
- (Exam Topic 4)
According to out of the box SmartEvent policy, which blade will automatically be correlated into events?

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

Answer: C

NEW QUESTION 548
- (Exam Topic 4)
Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 549
- (Exam Topic 4)
What does the Log "Views" tab show when SmartEvent is Correlating events?

A. A list of common reports
B. Reports for customization
C. Top events with charts and graphs
D. Details of a selected logs

Answer: D

NEW QUESTION 552
- (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 555
- (Exam Topic 4)
Which of the following statements about SecureXL NAT Templates is true?

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

Answer: A

NEW QUESTION 560
- (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 564
- (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 567
- (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 568
- (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 572
- (Exam Topic 4)

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	Any	Any	Any	NBT	Drop	None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	Any	Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	Any	Any	dns	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	Any	Any	http https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	Any	ftp AP-Defender	Accept	Log	Policy Targets
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.
What does this mean?

A. This rule N
B. 6 has been marked for deletion in your Management session.
C. This rule N
D. 6 has been marked for deletion in another Management session.
E. This rule N
F. 6 has been marked for editing in your Management session.
G. This rule N
H. 6 has been marked for editing in another Management session.

Answer: C

NEW QUESTION 577
- (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 580
- (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 581
- (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 584
- (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 589
- (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 591
- (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 596
- (Exam Topic 4)
What are the two high availability modes?

A. Load Sharing and Legacy
B. Traditional and New
C. Active and Standby
D. New and Legacy

Answer: D

Explanation:
ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION 598
- (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 599
- (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 604
- (Exam Topic 4)
What is the command used to activated Multi-Version Cluster mode?

A. set cluster member mvc on in Clish
B. set mvc on on Clish
C. set cluster MVC on in Expert Mode
D. set cluster mvc on in Expert Mode

Answer: A

NEW QUESTION 608
- (Exam Topic 4)
Which member of a high-availability cluster should be upgraded first in a Zero downtime upgrade?

A. The Standby Member
B. The Active Member
C. The Primary Member
D. The Secondary Member

Answer: A

NEW QUESTION 609
- (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 610
- (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 614
- (Exam Topic 4)
You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. Right click Accept in the rule, select “More”, and then check ‘Enable Identity Captive Portal’.
B. On the firewall object, Legacy Authentication screen, check ‘Enable Identity Captive Portal’.
C. In the Captive Portal screen of Global Properties, check ‘Enable Identity Captive Portal’.
D. On the Security Management Server object, check the box ‘Identity Logging’.

Answer: A

NEW QUESTION 617
- (Exam Topic 4)
What Is the difference between Updatable Objects and Dynamic Objects

A. Dynamic Objects ate maintained automatically by the Threat Clou
B. Updatable Objects are created and maintained locall
C. In both cases there is no need to install policy for the changes to take effect.
D. Updatable Objects is a Threat Cloud Servic
E. The provided Objects are updated automaticall
F. Dynamic Objects are created and maintained locally For Dynamic Objectsthere is no need to install policy for the changes to take effect.
G. Updatable Objects is a Threat Cloud Servic
H. The provided Objects are updated automaticall
I. Dynamic Objects are created and maintained locally In both cases there is noneed to install policy for the changes to take effect.
J. Dynamic Objects are maintained automatically by the Threat Clou
K. For Dynamic Objects there rs no need to install policy for the changes to take effec
L. Updatable Objects are created and maintained locally.

Answer: B

NEW QUESTION 622
- (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 623
- (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 624
- (Exam Topic 4)
What is the minimum number of CPU cores required to enable CoreXL?

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

Answer: C

Explanation:
Default number of CoreXL IPv4 FW instances:
Note: The real number of CoreXL FW instances depends on the current CoreXL license. Number of
CPU cores Default number of CoreXL IPv4
FW instances Default number of Secure Network Distributors (SNDs)
1 1
Note: CoreXL is disabled 0 Note: CoreXL is disabled
2 2 2
4 3 1
6 - 20 [Number of CPU cores] - 2 2
More than 20 (1) [Number of CPU cores] - 4 4

NEW QUESTION 629
- (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 630
- (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 632
- (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 634
- (Exam Topic 4)
Joey want to configure NTP on R81 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

A. https://<Device_IP_Adress>
B. http://<Device IP_Address>:443
C. https://<Device_IP_Address>:10000
D. https://<Device_IP_Address>:4434

Answer: A

NEW QUESTION 639
- (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 641
- (Exam Topic 4)
How is communication between different Check Point components secured in R81? As with all questions, select the BEST answer.

A. By using IPSEC
B. By using SIC
C. By using ICA
D. By using 3DES

Answer: B

NEW QUESTION 644
- (Exam Topic 4)
Which command shows only the table names of all kernel tables?

A. fwtab-t
B. fw tab -s
C. fw tab -n
D. fw tab -k

Answer: A

NEW QUESTION 648
- (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 650
- (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 654
- (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 659
- (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 660
- (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 663
- (Exam Topic 4)
Besides fw monitor, what is another command that can be used to capture packets?

A. arp
B. traceroute
C. tcpdump
D. ping

Answer: C

NEW QUESTION 664
- (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 665
- (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 667
- (Exam Topic 4)
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 669
- (Exam Topic 4)
Main Mode in IKEv1 uses how many packages for negotiation?

A. 4
B. depends on the make of the peer gateway
C. 3
D. 6

Answer: C

NEW QUESTION 671
- (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 672
- (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 677
- (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 678

- (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 682
- (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 686
- (Exam Topic 4)
When performing a minimal effort upgrade, what will happen to the network traffic?

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

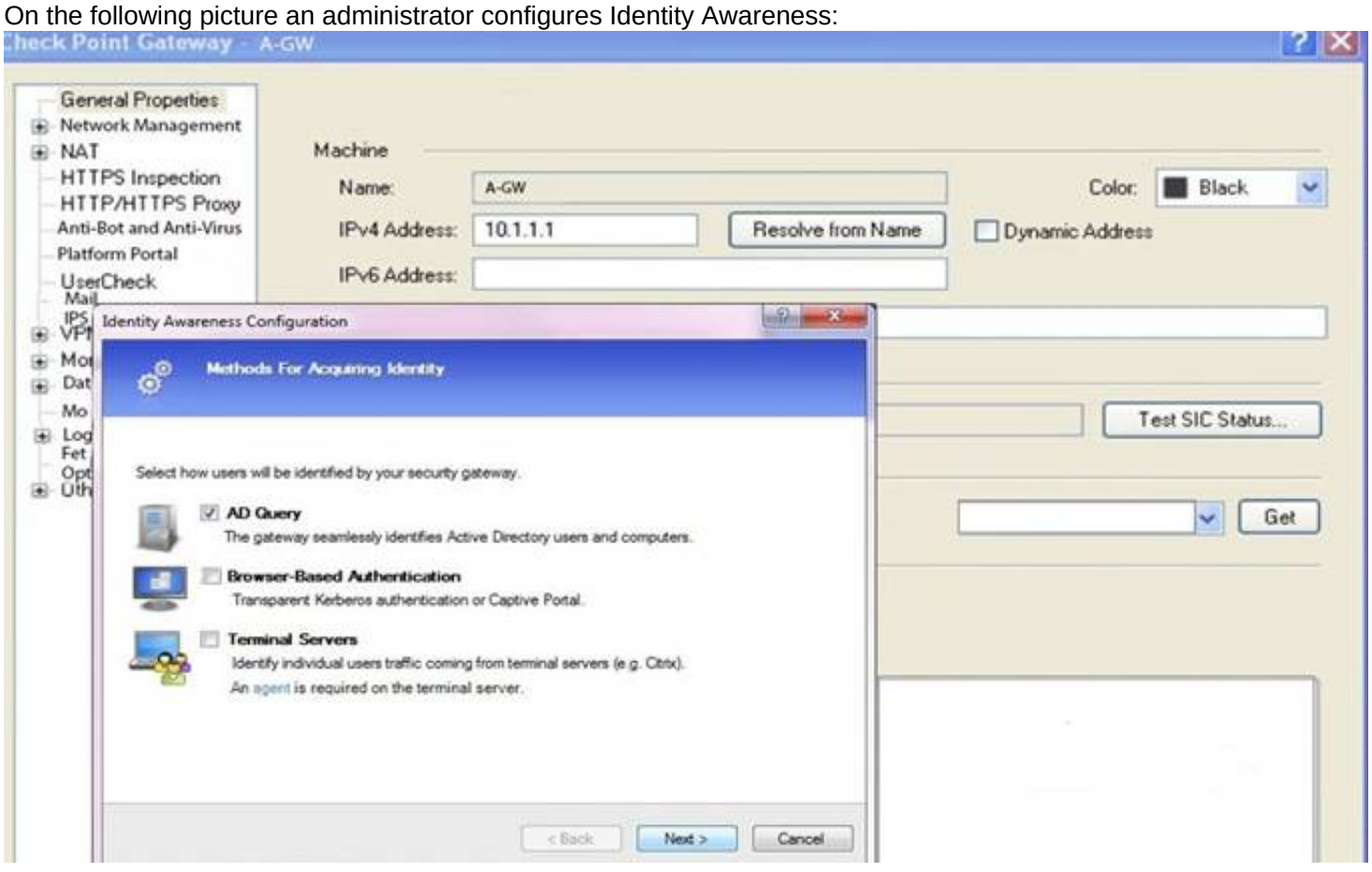
Answer: B

NEW QUESTION 691
- (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 695
- (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 698
- (Exam Topic 4)
How can you see historical data with cpview?

A. cpview -f <timestamp>
B. cpview -e <timestamp>
C. cpview -t <timestamp>
D. cpview -d <timestamp>

Answer: C

NEW QUESTION 702
- (Exam Topic 4)
In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?

A. If the Action of the matching rule is Accept the gateway will drop the packet
B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down
C. If the Action of the matching rule is Drop the gateway stops matching against later rules in the Policy Rule Base and drops the packet
D. If the rule does not matched in the Network policy it will continue to other enabled polices

Answer: C

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

NEW QUESTION 703
- (Exam Topic 4)
What destination versions are supported for a Multi-Version Cluster Upgrade?

A. R81.40 and later
B. R76 and later
C. R70 and Later
D. R81.10 and Later

Answer: D

NEW QUESTION 705
- (Exam Topic 4)
The log server sends what to the Correlation Unit?

A. Authentication requests
B. CPMI dbsync
C. Logs
D. Event Policy

Answer: C

NEW QUESTION 709
- (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 711
- (Exam Topic 4)
You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

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

Answer: A

NEW QUESTION 714
- (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 719
- (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 721
- (Exam Topic 4)
To optimize Rule Base efficiency, the most hit rules should be where?

A. Removed from the Rule Base.
B. Towards the middle of the Rule Base.
C. Towards the top of the Rule Base.
D. Towards the bottom of the Rule Base.

Answer: C

NEW QUESTION 724
- (Exam Topic 4)
What is the amount of Priority Queues by default?

A. There are 8 priority queues and this number cannot be changed.
B. There is no distinct number of queues since it will be changed in a regular basis based on its system requirements.
C. There are 7 priority queues by default and this number cannot be changed.
D. There are 8 priority queues by default, and up to 8 additional queues can be manually configured

Answer: D

NEW QUESTION 728
- (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 730
- (Exam Topic 4)
What command is used to manually failover a cluster during a zero downtime upgrade?

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

Answer: C

NEW QUESTION 733
- (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 738
- (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 739
- (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 743
- (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 744
- (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 749
- (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 752
- (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 753
- (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 755
- (Exam Topic 4)
Which command shows the current Security Gateway Firewall chain?

A. show current chain
B. show firewall chain
C. fw ctl chain
D. fw ctl firewall-chain

Answer: C

NEW QUESTION 756
- (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 760
- (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 IoC XMfcfile and analysis of SOLR documents

Answer: D

NEW QUESTION 762
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-315.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-315.81 Product From:

https://www.2passeasy.com/dumps/156-315.81/

Money Back Guarantee

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