CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

NEW QUESTION 1
- (Exam Topic 1)
Which is NOT an example of a Check Point API?

A. Gateway API
B. Management API
C. OPSC SDK
D. Threat Prevention API

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?

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

Answer: B

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
Which of these statements describes the Check Point ThreatCloud?

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

Answer: D

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
Check Pont Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____.

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

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) _____ or _____ action for the file types.

A. Inspect/Bypass
B. Inspect/Prevent

C. Prevent/Bypass
D. Detect/Bypass

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
Which command collects diagnostic data for analyzing customer setup remotely?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 1)
What has to be taken into consideration when configuring Management HA?

A. The Database revisions will not be synchronized between the management servers
B. SmartConsole must be closed prior to synchronized changes in the objects database
C. If you wanted to use Full Connectivity Upgrade, you must change the Implied Rules to allow FW1_cpredundant to pass before the Firewall Control Connections.
D. For Management Server synchronization, only External Virtual Switches are supporte
E. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.

Answer: A

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

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

Answer: C

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

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

Answer: C

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

NEW QUESTION 13
- (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 14
- (Exam Topic 1)
What is the least amount of CPU cores required to enable CoreXL?

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

Answer: A

NEW QUESTION 15
- (Exam Topic 1)
Which CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat
B. ips pstats reset
C. ips pmstats refresh
D. ips pmstats reset

Answer: D

NEW QUESTION 16
- (Exam Topic 1)
Which command can you use to verify the number of active concurrent connections?

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

Answer: B

NEW QUESTION 17
- (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 19
- (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 24
- (Exam Topic 1)
Fill in the blank: The command _____ provides the most complete restoration of a R81 configuration.

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

Answer: A

NEW QUESTION 29
- (Exam Topic 1)
What is the mechanism behind Threat Extraction?

A. This a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender.
B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient.
C. This is a new mechanism to identify the IP address of the sender of malicious codes and put it into the SAM database (Suspicious Activity Monitoring).

D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast.

Answer: D

NEW QUESTION 34
- (Exam Topic 1)
Which command will allow you to see the interface status?

A. cphaprob interface
B. cphaprob –I interface
C. cphaprob –a if
D. cphaprob stat

Answer: C

NEW QUESTION 37
- (Exam Topic 1)
On R81.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

A. 18210
B. 18184
C. 257
D. 18191

Answer: B

NEW QUESTION 40
- (Exam Topic 1)
What Factor preclude Secure XL Templating?

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

Answer: A

NEW QUESTION 41
- (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 42
- (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 45
- (Exam Topic 1)
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

A. UDP port 265
B. TCP port 265
C. UDP port 256
D. TCP port 256

Answer: D

Explanation:
Synchronization works in two modes:
Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP

connection on port 256.
Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by the Security Gateway kernel using UDP connections on port 8116.

NEW QUESTION 46
- (Exam Topic 1)
There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?

A. Using Web Services
B. Using Mgmt_cli tool
C. Using CLISH
D. Using SmartConsole GUI console
E. Events are collected with SmartWorkflow from Trouble Ticket systems

Answer: E

NEW QUESTION 50
- (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 53
- (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 56
- (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 58
- (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 60
- (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 63
- (Exam Topic 1)
Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 67
- (Exam Topic 1)
What is the limitation of employing Sticky Decision Function?

A. With SDF enabled, the involved VPN Gateways only supports IKEv1
B. Acceleration technologies, such as SecureXL and CoreXL are disabled when activating SDF
C. With SDF enabled, only ClusterXL in legacy mode is supported
D. With SDF enabled, you can only have three Sync interfaces at most

Answer: B

NEW QUESTION 68
- (Exam Topic 1)
What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

A. Anti-Bot is the only countermeasure against unknown malware
B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
C. Anti-Bot is the only signature-based method of malware protection.
D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.

Answer: D

NEW QUESTION 72
- (Exam Topic 1)
Tom has been tasked to install Check Point R81 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

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

Answer: C

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

NEW QUESTION 76
- (Exam Topic 1)
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode

Answer: C

Explanation:
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

NEW QUESTION 79
- (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 84
- (Exam Topic 1)
If you needed the Multicast MAC address of a cluster, what command would you run?

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

Answer: D

NEW QUESTION 85
- (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 89
- (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 94
- (Exam Topic 1)
Connections to the Check Point R81 Web API use what protocol?

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

Answer: A

NEW QUESTION 99
- (Exam Topic 1)
Which of the following type of authentication on Mobile Access can NOT be used as the first authentication method?

A. Dynamic ID
B. RADIUS
C. Username and Password
D. Certificate

Answer: A

NEW QUESTION 102
- (Exam Topic 1)
In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?

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

Answer: A

NEW QUESTION 107
- (Exam Topic 1)
Which of the following statements is TRUE about R81 management plug-ins?

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

Answer: C

NEW QUESTION 112
- (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 114
- (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 115
- (Exam Topic 1)
Which method below is NOT one of the ways to communicate using the Management API's?

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

Answer: D

NEW QUESTION 116
- (Exam Topic 1)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 118
- (Exam Topic 1)
What command verifies that the API server is responding?

A. api stat
B. api status
C. show api_status
D. app_get_status

Answer: B

NEW QUESTION 121
- (Exam Topic 1)
What is true about VRRP implementations?

A. VRRP membership is enabled in cpconfig
B. VRRP can be used together with ClusterXL, but with degraded performance
C. You cannot have a standalone deployment
D. You cannot have different VRIDs in the same physical network

Answer: C

NEW QUESTION 123
- (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 128
- (Exam Topic 2)
What are the blades of Threat Prevention?

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

Answer: D

NEW QUESTION 132
- (Exam Topic 2)
John is using Management HA. Which Smartcenter should be connected to for making changes?

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

Answer: B

NEW QUESTION 136
- (Exam Topic 2)
Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

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

Answer: C

NEW QUESTION 138
- (Exam Topic 2)
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 143
- (Exam Topic 2)
Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

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

Answer: D

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

NEW QUESTION 145
- (Exam Topic 2)
An administrator would like to troubleshoot why templating is not working for some traffic. How can he determine at which rule templating is disabled?

A. He can use the fw accel stat command on the gateway.
B. He can use the fw accel statistics command on the gateway.
C. He can use the fwaccel stat command on the Security Management Server.
D. He can use the fwaccel stat command on the gateway

Answer: D

NEW QUESTION 149
- (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 151
- (Exam Topic 2)
You need to see which hotfixes are installed on your gateway, which command would you use?

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

Answer: D

NEW QUESTION 155
- (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 159
- (Exam Topic 2)
Under which file is the proxy arp configuration stored?

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

Answer: D

NEW QUESTION 164
- (Exam Topic 2)
Which of the following will NOT affect acceleration?

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

Answer: B

NEW QUESTION 165
- (Exam Topic 2)
What is the protocol and port used for Health Check and State Synchronization in ClusterXL?

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

Answer: C

NEW QUESTION 166
- (Exam Topic 2)
Can multiple administrators connect to a Security Management Server at the same time?

A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time

C. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
D. Yes, but only one has the right to write.

Answer: C

NEW QUESTION 171
- (Exam Topic 2)
For Management High Availability, which of the following is NOT a valid synchronization status?

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

Answer: B

NEW QUESTION 175
- (Exam Topic 2)
What is the purpose of extended master key extension/session hash?

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

Answer: B

NEW QUESTION 178
- (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 179
- (Exam Topic 2)
You have existing dbedit scripts from R77. Can you use them with R81.10?

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

Answer: D

NEW QUESTION 180
- (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 182
- (Exam Topic 2)
Please choose correct command to add an "emailserver1" host with IP address 10.50.23.90 using GAiA management CLI?

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

Answer: D

NEW QUESTION 186
- (Exam Topic 2)
Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

A. enable DLP and select.exe and .bat file type
B. enable .exe & .bat protection in IPS Policy
C. create FW rule for particular protocol
D. tecli advanced attributes set prohibited_file_types exe.bat

Answer: A

NEW QUESTION 190
- (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 191
- (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 194
- (Exam Topic 2)
Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 196
- (Exam Topic 2)
What are the main stages of a policy installations?

A. Verification & Compilation, Transfer and Commit
B. Verification & Compilation, Transfer and Installation
C. Verification, Commit, Installation
D. Verification, Compilation & Transfer, Installation

Answer: A

NEW QUESTION 200
- (Exam Topic 2)
What is mandatory for ClusterXL to work properly?

A. The number of cores must be the same on every participating cluster node
B. The Magic MAC number must be unique per cluster node
C. The Sync interface must not have an IP address configured
D. If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on all cluster members

Answer: B

NEW QUESTION 201
- (Exam Topic 2)
What scenario indicates that SecureXL is enabled?

A. Dynamic objects are available in the Object Explorer

B. SecureXL can be disabled in cpconfig
C. fwaccel commands can be used in clish
D. Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 205
- (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 210
- (Exam Topic 2)
Which Remote Access Client does not provide an Office-Mode Address?

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

Answer: A

NEW QUESTION 211
- (Exam Topic 2)
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported

Answer: A

NEW QUESTION 214
- (Exam Topic 2)
Which one of the following is true about Threat Extraction?

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

Answer: A

NEW QUESTION 215
- (Exam Topic 2)
With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users
can perform the applications. Mobile Access encrypts all traffic using:

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

Answer: A

NEW QUESTION 217
- (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 222
- (Exam Topic 2)
When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?

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

Answer: C

NEW QUESTION 227
- (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 228
- (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 233
- (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 238
- (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 243
- (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 248
- (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 253
- (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 255
- (Exam Topic 2)
Which one of the following is true about Threat Emulation?

A. Takes less than a second to complete
B. Works on MS Office and PDF files only
C. Always delivers a file
D. Takes minutes to complete (less than 3 minutes)

Answer: D

NEW QUESTION 260
- (Exam Topic 2)
Which command gives us a perspective of the number of kernel tables?

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

Answer: B

NEW QUESTION 263
- (Exam Topic 2)
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 264
- (Exam Topic 2)
After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

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

Answer: B

NEW QUESTION 266
- (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 269
- (Exam Topic 3)
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 271
- (Exam Topic 3)
What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 274
- (Exam Topic 3)
Which SmartConsole tab is used to monitor network and security performance?

A. Manage Setting
B. Security Policies
C. Gateway and Servers
D. Logs and Monitor

Answer: D

NEW QUESTION 279
- (Exam Topic 3)
The essential means by which state synchronization works to provide failover in the event an active member goes down, _____ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

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

Answer: A

NEW QUESTION 283
- (Exam Topic 3)
Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.
What will happen to the changes already made?

A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.
B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
C. Tom's changes will be lost since he lost connectivity and he will have to start again.
D. Tom will have to reboot his SmartConsole computer, clear to cache, and restore changes.

Answer: A

NEW QUESTION 287
- (Exam Topic 3)
To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

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

Answer: D

NEW QUESTION 289
- (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 294
- (Exam Topic 3)
Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?

A. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses
B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
C. The CoreXL FW instances assignment mechanism is based on IP Protocol type
D. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type

Answer: B

NEW QUESTION 296
- (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 297
- (Exam Topic 3)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 300
- (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 304
- (Exam Topic 3)
Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?

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

Answer: D

NEW QUESTION 305
- (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 308
- (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 313
- (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 318
- (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 323
- (Exam Topic 3)
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned O
B. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OF
D. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
E. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
F. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

Answer: A

NEW QUESTION 326
- (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 331
- (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 332
- (Exam Topic 3)
One of major features in R81 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

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

Answer: C

NEW QUESTION 337
- (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 342
- (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 345
- (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 348
- (Exam Topic 3)
SandBlast agent extends 0 day prevention to what part of the network?

A. Web Browsers and user devices
B. DMZ server
C. Cloud
D. Email servers

Answer: A

NEW QUESTION 349
- (Exam Topic 3)
What command lists all interfaces using Multi-Queue?

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

Answer: A

NEW QUESTION 352
- (Exam Topic 3)
What kind of information would you expect to see using the sim affinity command?

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

Answer: D

NEW QUESTION 353
- (Exam Topic 3)
What CLI command compiles and installs a Security Policy on the target's Security Gateways?

A. fwm compile
B. fwm load
C. fwm fetch
D. fwm install

Answer: B

NEW QUESTION 357
- (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 361
- (Exam Topic 3)
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

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

Answer: B

NEW QUESTION 365
- (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 370
- (Exam Topic 3)
Which of the following commands shows the status of processes?

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

Answer: D

NEW QUESTION 371
- (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 372

- (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 377
- (Exam Topic 3)
What is the SandBlast Agent designed to do?

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

Answer: C

NEW QUESTION 380
- (Exam Topic 3)
When using CPSTAT, what is the default port used by the AMON server?

A. 18191
B. 18192
C. 18194
D. 18190

Answer: B

NEW QUESTION 381
- (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 385
- (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 386
- (Exam Topic 3)
What will be the effect of running the following command on the Security Management Server?
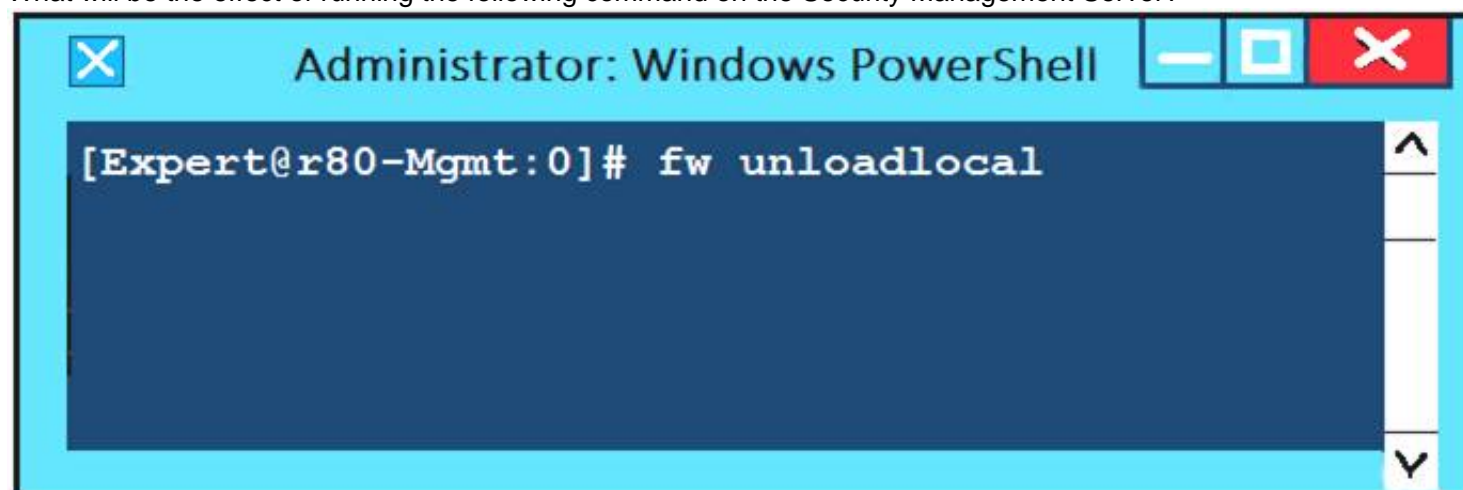
A. Remove the installed Security Policy.
B. Remove the local ACL lists.
C. No effect.
D. Reset SIC on all gateways.

Answer: A

NEW QUESTION 389
- (Exam Topic 3)
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

Answer: D

NEW QUESTION 393
- (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 395
- (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 398
- (Exam Topic 3)
Which command would you use to set the network interfaces' affinity in Manual mode?

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

Answer: D

NEW QUESTION 399
- (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 401
- (Exam Topic 3)
When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

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

Answer: D

NEW QUESTION 402
- (Exam Topic 3)
For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

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

Answer: D

NEW QUESTION 403
- (Exam Topic 3)
What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?

A. 4 Interfaces – an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
B. 3 Interfaces – an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
C. 1 Interface – an interface leading to the organization and the Internet, and configure for synchronization.
D. 2 Interfaces – a data interface leading to the organization and the Internet, a second interface for synchronization.

Answer: B

NEW QUESTION 407
- (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 412
- (Exam Topic 3)
What is the valid range for VRID value in VRRP configuration?

A. A.-1 - 254B.1 - 255C.0 - 254D.0 - 255

Answer: B

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

NEW QUESTION 414
- (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 418
- (Exam Topic 3)
You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

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

Answer: A

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

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

Answer: B

NEW QUESTION 424
- (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 428
- (Exam Topic 4)
How would you enable VMAC Mode in ClusterXL?

A. Cluster Object -> Edit -> ClusterXL and VRRP -> Use Virtual MAC
B. fw ctl set int vmac_mode 1
C. cphaconf vmac_mode set 1
D. Cluster Object -> Edit -> Cluster Members -> Edit -> Use Virtual MAC

Answer: A

Explanation:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal? eventSubmit_doGoviewsolutiondetails=&solutionid=sk50840

NEW QUESTION 433
- (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 434
- (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 435
- (Exam Topic 4)
Which components allow you to reset a VPN tunnel?

A. vpn tu command or SmartView monitor
B. delete vpn ike sa or vpn she11 command

C. vpn tunnelutil or delete vpn ike sa command
D. SmartView monitor only

Answer: D

NEW QUESTION 440
- (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 445
- (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 446
- (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 448
- (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 449
- (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 450
- (Exam Topic 4)
Which of the following Check Point commands is true to enable Multi-Version Cluster (MVC)?

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

Answer: D

NEW QUESTION 454
- (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 458
- (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 459
- (Exam Topic 4)
In R81, where do you manage your Mobile Access Policy?

A. Access Control Policy
B. Through the Mobile Console
C. Shared Gateways Policy
D. From the Dedicated Mobility Tab

Answer: B

NEW QUESTION 460
- (Exam Topic 4)
The customer has about 150 remote access user with a Windows laptops. Not more than 50 Clients will be connected at the same time. The customer want to use multiple VPN Gateways as entry point and a personal firewall. What will be the best license for him?

A. He will need Capsule Connect using MEP (multiple entry points).
B. Because the customer uses only Windows clients SecuRemote will be sufficient and no additional license is needed
C. He will need Harmony Endpoint because of the personal firewall.
D. Mobile Access license because he needs only a 50 user license, license count is per concurrent use

Answer: D

NEW QUESTION 462
- (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 465
- (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 466
- (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 470

- (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 471

- (Exam Topic 4)
Alice & Bob are concurrently logged In via SSH on the same Check Point Security Gateway as user "admin* however Bob was first logged in and acquired the lock Alice Is not aware that Bob is also togged in to the same Security Management Server as she is but she needs to perform very urgent configuration changes - which of the following GAIAclish command is true for overriding Bobs configuration database lock:

A. lock database override
B. unlock override database
C. unlock database override
D. database unlock override

Answer: A

NEW QUESTION 472

- (Exam Topic 4)
Choose the correct syntax to add a new host named "emailserver1" with IP address 10.50.23.90 using GAiA Management CLI?

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

Answer: D

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

NEW QUESTION 473

- (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 476

- (Exam Topic 4)
In Threat Prevention, you can create new or clone profiles but you CANNOT change the out-of-the-box profiles of:

A. Basic, Optimized, Strict
B. Basic, Optimized, Severe
C. General, Escalation, Severe
D. General, purposed, Strict

Answer: A

NEW QUESTION 477

- (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 480
- (Exam Topic 4)
Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

A. cpexport
B. sysinfo
C. cpsizeme
D. cpinfo

Answer: D

NEW QUESTION 485
- (Exam Topic 4)
Which upgrade method you should use upgrading from R80.40 to R81.10 to avoid any downtime?

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

Answer: D

NEW QUESTION 490
- (Exam Topic 4)
The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits if the Track option is set to "None"?

A. No, it will work independentl
B. Hit Count will be shown only for rules Track option set as Log or alert.
C. Yes it will work independently as long as "analyze all rules" tick box is enabled on the Security Gateway.
D. No, it will not work independently because hit count requires all rules to be logged.
E. Yes it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways.

Answer: D

NEW QUESTION 492
- (Exam Topic 4)
You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways

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

Answer: C

NEW QUESTION 493
- (Exam Topic 4)
Within the Check Point Firewall Kernel resides Chain Modules, which are individually responsible for the inspection of a specific blade or feature that has been enabled in the configuration of the gateway. For Wire mode configuration, chain modules marked with _____ will not apply.

A. fffffff
B. 00000001
C. 00000002
D. 00000003

Answer: B

NEW QUESTION 497
- (Exam Topic 4)
When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

A. RADIUS
B. Remote Access and RADIUS
C. AD Query
D. AD Query and Browser-based Authentication

Answer: D

Explanation:
Identity Awareness gets identities from these acquisition sources:

NEW QUESTION 502
- (Exam Topic 4)
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

A. Pentagon
B. Combined
C. Meshed
D. Star

Answer: D

NEW QUESTION 504
- (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 505
- (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 506
- (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 511
- (Exam Topic 4)
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____.

A. On all satellite gateway to satellite gateway tunnels
B. On specific tunnels for specific gateways
C. On specific tunnels in the community
D. On specific satellite gateway to central gateway tunnels

Answer: C

NEW QUESTION 515
- (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 518
- (Exam Topic 4)
Which of the following is NOT an internal/native Check Point command?

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

Answer: C

NEW QUESTION 521
- (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 524
- (Exam Topic 4)
How many versions, besides the destination version, are supported in a Multi-Version Cluster Upgrade?
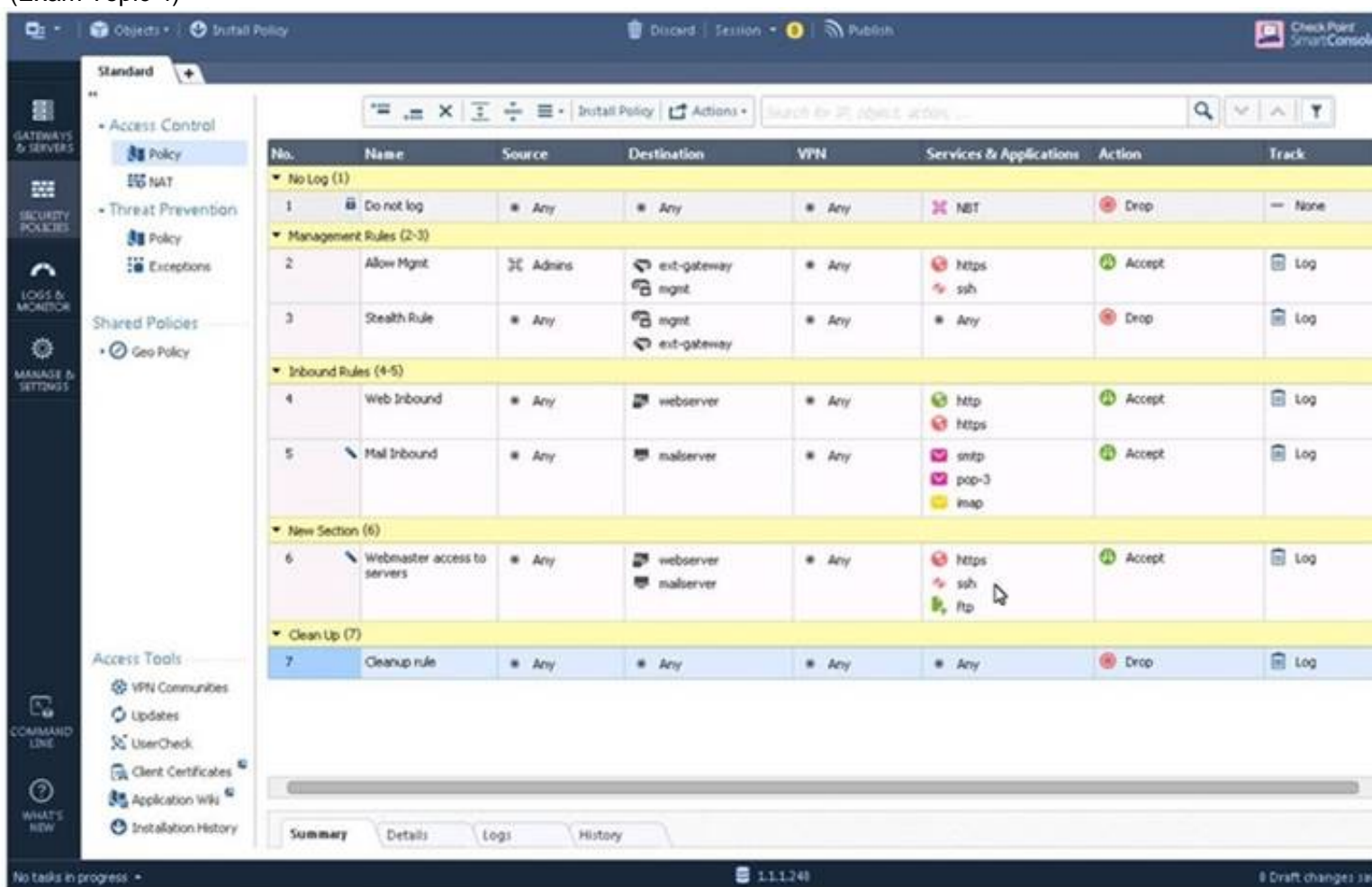
A. 1
B. 3
C. 2
D. 4

Answer: B

NEW QUESTION 526
- (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 531
- (Exam Topic 4)
What feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?

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

Answer: B

NEW QUESTION 536
- (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 539
- (Exam Topic 4)
By default how often updates are checked when the CPUSE Software Updates Policy is set to Automatic?

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

Answer: D

Explanation:

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

NEW QUESTION 543
- (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 548
- (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 549
- (Exam Topic 4)
Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 550
- (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 551
- (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 554
- (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 557
- (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 558
- (Exam Topic 4)
What should the admin do in case the Primary Management Server is temporary down?

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

Answer: A

NEW QUESTION 560
- (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 562
- (Exam Topic 4)
Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

A. cpm
B. fwd

C. cpd
D. fwmD18912E1457D5D1DDCBD40AB3BF70D5D

Answer: D

NEW QUESTION 563
- (Exam Topic 4)
Which command is used to obtain the configuration lock in Gaia?

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

Answer: A

Explanation:
Obtaining a Configuration Lock

NEW QUESTION 568
- (Exam Topic 4)
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 569
- (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 572
- (Exam Topic 4)
Which component is NOT required to communicate with the Web Services API?

A. API key
B. session ID token
C. content-type
D. Request payload

Answer: A

NEW QUESTION 577
- (Exam Topic 4)
What is the default shell for the command line interface?

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

Answer: B

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

NEW QUESTION 578
- (Exam Topic 4)
John is using Management HA. Which Security Management Server should he use for making changes?

A. secondary Smartcenter
B. active SmartConsole
C. connect virtual IP of Smartcenter HA

D. primary Log Server

Answer: B

NEW QUESTION 583
- (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 584
- (Exam Topic 4)
What is the default shell of Gaia CLI?

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

Answer: B

NEW QUESTION 585
- (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 589
- (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 594
- (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 599
- (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 602
- (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 603
- (Exam Topic 4)
When synchronizing clusters, which of the following statements is FALSE?

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

Answer: D

NEW QUESTION 607
- (Exam Topic 4)
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

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

Answer: D

NEW QUESTION 610
- (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 613
- (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 615
- (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 616
- (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 620
- (Exam Topic 4)
True or False: In R81, more than one administrator can login to the Security Management Server with write permission at the same time.

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

Answer: B

NEW QUESTION 621
- (Exam Topic 4)
The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?

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

Answer: C

NEW QUESTION 622
- (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 625
- (Exam Topic 4)
What is the benefit of Manual NAT over Automatic NAT?

A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy.
B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
C. You have the full control about the priority of the NAT rules
D. On IPSO and GAIA Gateways, it is handled in a stateful manner

Answer: C

NEW QUESTION 630
- (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 635
- (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 638
- (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 640
- (Exam Topic 4)
Is it possible to establish a VPN before the user login to the Endpoint Client?

A. yes, you had to set neo_remember_user_password to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_remember_user_passwordattribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway
B. no, the user must login first.
C. ye
D. you had to set neo_always_connected to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_always_connected attribute in thetrac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway
E. yes, you had to enable Machine Authentication in the Gateway object of the Smart Console

Answer: D

NEW QUESTION 645
- (Exam Topic 4)
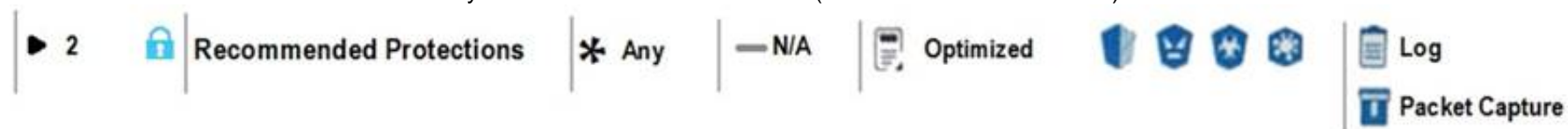Which one is not a valid Package Option In the Web GUI for CPUSE?

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

Answer: B

NEW QUESTION 649
- (Exam Topic 4)
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)

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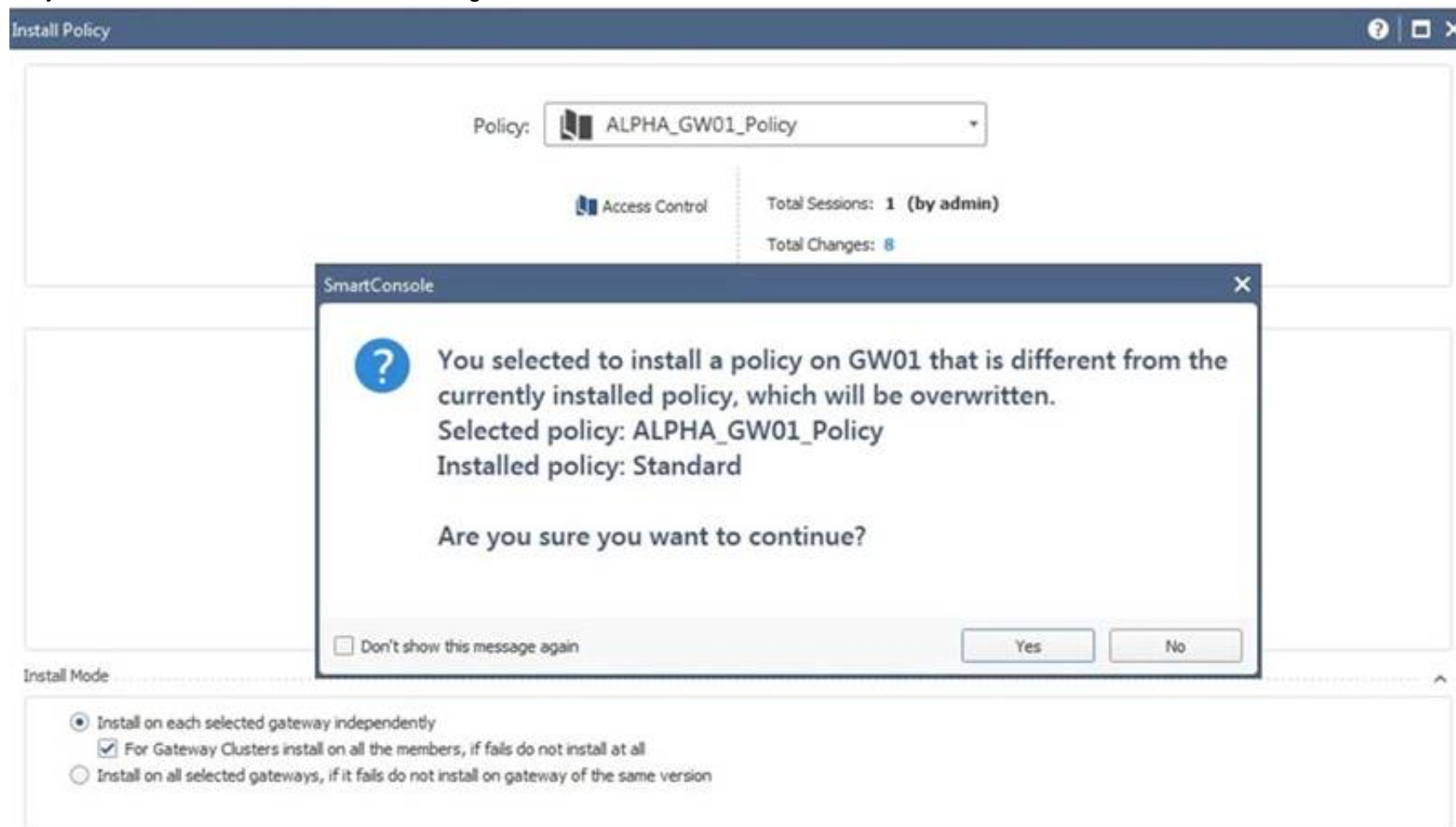
Answer: B

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

NEW QUESTION 651
- (Exam Topic 4)
Why would an administrator see the message below?

A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 654
- (Exam Topic 4)
What state is the Management HA in when both members have different policies/databases?

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

Answer: D

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

NEW QUESTION 659
- (Exam Topic 4)
Which of the following processes pulls the application monitoring status from gateways?

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

Answer: A

NEW QUESTION 664
- (Exam Topic 4)
What is false regarding prerequisites for the Central Deployment usage?

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

Answer: D

NEW QUESTION 666

- (Exam Topic 4)
What API command below creates a new host object with the name "My Host" and IP address of "192 168 0 10"?

A. set host name "My Host" ip-address "192.168.0.10"
B. new host name "My Host" ip-address "192 168.0.10"
C. create host name "My Host" ip-address "192.168 0.10"
D. mgmt.cli -m <mgmt ip> add host name "My Host" ip-address "192.168.0 10"

Answer: A

NEW QUESTION 668
- (Exam Topic 4)
While using the Gaia CLI. what is the correct command to publish changes to the management server?

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

Answer: B

NEW QUESTION 671
- (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 673
- (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?
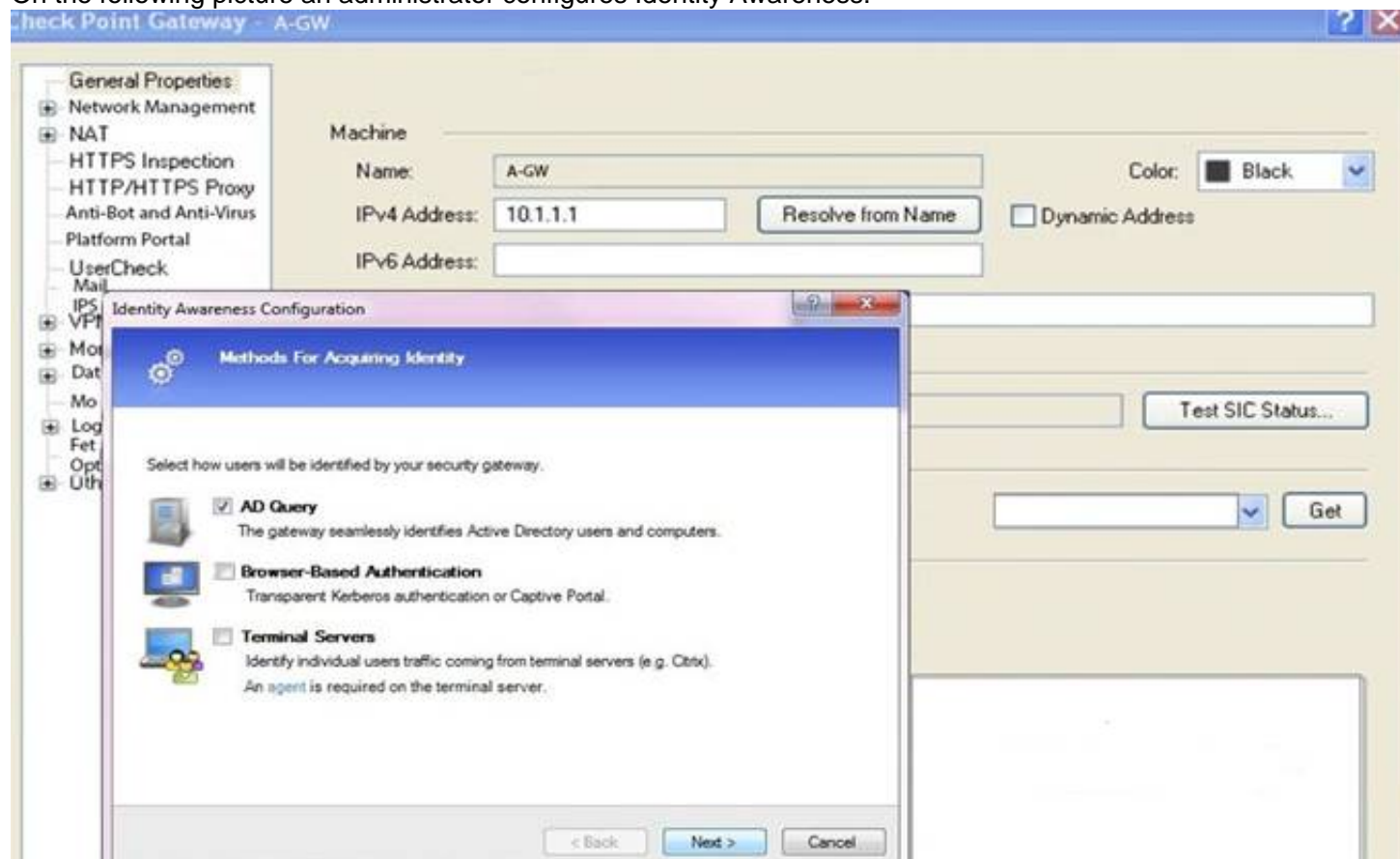
A. Ask
B. Drop
C. Inform
D. Reject

Answer: D

NEW QUESTION 677
- (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 678
- (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 681
- (Exam Topic 4)
What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

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

Answer: B

NEW QUESTION 683
- (Exam Topic 4)
What is the recommended way to have a redundant Sync connection between the cluster nodes?

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

Answer: C

NEW QUESTION 684
- (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 689
- (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 693
- (Exam Topic 4)
What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

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

Answer: C

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

NEW QUESTION 697
- (Exam Topic 4)
Aaron is a Syber Security Engineer working for Global Law Firm with large scale deployment of Check Point Enterprise Appliances running GAiA R81.X The Network Security Developer Team is having an issue testing the API with a newly deployed R81.X Security Management Server Aaron wants to confirm API services are working properly. What should he do first?

A. Aaron should check API Server status with "fwm api status" from Expert mode If services are stopped, he should start them with "fwm api start".
B. Aaron should check API Server status with "cpapi status" from Expert mod
C. If services are stopped, he should start them with "cpapi start"
D. Aaron should check API Server status with "api status" from Expert mode If services are stopped, he should start them with "api start"
E. Aaron should check API Server status with "cpm api status" from Expert mod
F. If services are stopped, he should start them with "cpi api start".

Answer: C

NEW QUESTION 698
- (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 702
- (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 705
- (Exam Topic 4)
When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

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

Answer: C

NEW QUESTION 707
- (Exam Topic 4)
What are possible Automatic Reactions in SmartEvent?

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

Answer: A

NEW QUESTION 708
- (Exam Topic 4)
What is "Accelerated Policy Installation"?

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

Answer: C

NEW QUESTION 711
- (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 714
- (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 717
- (Exam Topic 4)
Which Check Point software blade provides protection from zero-day and undiscovered threats?

A. Firewall
B. Threat Emulation
C. Application Control
D. Threat Extraction

Answer: B

NEW QUESTION 722
- (Exam Topic 4)
Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

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

Answer: D

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

NEW QUESTION 726
- (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 730
- (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 732
- (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 733
- (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 738
- (Exam Topic 4)
The "MAC magic" value must be modified under the following condition:

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

Answer: D

NEW QUESTION 739
- (Exam Topic 4)
Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .

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

Answer: C

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

NEW QUESTION 743
- (Exam Topic 4)
If a "ping"-packet is dropped by FW1 Policy –on how many inspection Points do you see this packet in "fw monitor"?

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

Answer: C

NEW QUESTION 746
- (Exam Topic 4)
Fill in the blank: Authentication rules are defined for _____ .

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

Answer: A

NEW QUESTION 749
- (Exam Topic 4)
By default, which port does the WebUI listen on?

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

Answer: C

NEW QUESTION 751
- (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 752
- (Exam Topic 4)
What are the two types of tests when using the Compliance blade?

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

Answer: D

NEW QUESTION 757
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

156-315.81 Practice Exam Features:

* 156-315.81 Questions and Answers Updated Frequently

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

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

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

100% Actual & Verified — Instant Download, Please Click
[Order The 156-315.81 Practice Test Here](https://www.certshared.com/exam/156-315.81/)