CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

NEW QUESTION 1
- (Exam Topic 1)
What are the different command sources that allow you to communicate with the API server?

A. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
B. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
C. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
D. API_cli Tool, Gaia CLI, Web Services

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
Which statement is true regarding redundancy?

A. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob –f if command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Machines in a ClusterXL High Availability configuration must be synchronized.
D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Answer: D

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
Which view is NOT a valid CPVIEW view?

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

Answer: C

NEW QUESTION 5
- (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 6
- (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 7
- (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 8
- (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 9
- (Exam Topic 1)
Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

A. 15 sec
B. 60 sec
C. 5 sec
D. 30 sec

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
In order to get info about assignment (FW, SND) of all CPUs in your SGW, what is the most accurate CLI command?

A. fw ctl sdstat
B. fw ctl affinity –l –a –r –v
C. fw ctl multik stat
D. cpinfo

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don’t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

Answer: C

NEW QUESTION 11
- (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 13
- (Exam Topic 1)
Which command can you use to enable or disable multi-queue per interface?

A. cpmq set
B. Cpmqueue set
C. Cpmq config
D. St cpmq enable

Answer: A

NEW QUESTION 16
- (Exam Topic 1)
Which CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat

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

Answer: D

NEW QUESTION 18
- (Exam Topic 1)
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 21
- (Exam Topic 1)
The Firewall kernel is replicated multiple times, therefore:

A. The Firewall kernel only touches the packet if the connection is accelerated
B. The Firewall can run different policies per core
C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
D. The Firewall can run the same policy on all cores.

Answer: D

Explanation:
On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

NEW QUESTION 23
- (Exam Topic 1)
The Security Gateway is installed on GAIA R81. The default port for the Web User Interface is _____.

A. TCP 18211
B. TCP 257
C. TCP 4433
D. TCP 443

Answer: D

NEW QUESTION 24
- (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 26
- (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 29
- (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 33
- (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 36
- (Exam Topic 1)
The Firewall Administrator is required to create 100 new host objects with different IP addresses. What API command can he use in the script to achieve the requirement?

A. add host name <New HostName> ip-address <ip address>
B. add hostname <New HostName> ip-address <ip address>
C. set host name <New HostName> ip-address <ip address>
D. set hostname <New HostName> ip-address <ip address>

Answer: A

NEW QUESTION 41
- (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 45
- (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 49
- (Exam Topic 1)
Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116
C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members.

Answer: A

NEW QUESTION 54
- (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 55
- (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 56
- (Exam Topic 1)
Identify the API that is not supported by Check Point currently.

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

Answer: C

NEW QUESTION 57
- (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 62
- (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 65
- (Exam Topic 1)
What is not a component of Check Point SandBlast?

A. Threat Emulation
B. Threat Simulator
C. Threat Extraction
D. Threat Cloud

Answer: B

NEW QUESTION 69
- (Exam Topic 1)
Which command lists all tables in Gaia?

A. fw tab –t
B. fw tab –list
C. fw-tab –s
D. fw tab -1

Answer: C

NEW QUESTION 71
- (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 76
- (Exam Topic 1)
Which two of these Check Point Protocols are used by SmartEvent Processes?

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

Answer: D

NEW QUESTION 79
- (Exam Topic 1)
How many images are included with Check Point TE appliance in Recommended Mode?

A. 2(OS) images
B. images are chosen by administrator during installation
C. as many as licensed for
D. the most new image

Answer: A

NEW QUESTION 83
- (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 85
- (Exam Topic 1)
Where you can see and search records of action done by R81 SmartConsole administrators?

A. In SmartView Tracker, open active log
B. In the Logs & Monitor view, select “Open Audit Log View”
C. In SmartAuditLog View
D. In Smartlog, all logs

Answer: B

NEW QUESTION 88
- (Exam Topic 1)
In R81 spoofing is defined as a method of:

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

Answer: D

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

NEW QUESTION 89
- (Exam Topic 1)
Which packet info is ignored with Session Rate Acceleration?

A. source port ranges
B. source ip
C. source port
D. same info from Packet Acceleration is used

Answer: B

NEW QUESTION 93
- (Exam Topic 1)
CoreXL is supported when one of the following features is enabled:

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

Answer: B

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

NEW QUESTION 95
- (Exam Topic 1)
What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

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

Answer: A

NEW QUESTION 98
- (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 100
- (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 105
- (Exam Topic 2)
Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

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

Answer: D

NEW QUESTION 107
- (Exam Topic 2)
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

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

Answer: A

NEW QUESTION 112
- (Exam Topic 2)
As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name ‘cover-company-logo.png’ and then copy that image file to which directory on the SmartEvent server?

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

Answer: C

NEW QUESTION 114
- (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 116
- (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 119
- (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 120
- (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 123
- (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 128
- (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 133
- (Exam Topic 2)
What information is NOT collected from a Security Gateway in a Cpinfo?

A. Firewall logs

B. Configuration and database files
C. System message logs
D. OS and network statistics

Answer: A

NEW QUESTION 137
- (Exam Topic 2)
What is the command to see cluster status in cli expert mode?

A. fw ctl stat
B. clusterXL stat
C. clusterXL status
D. cphaprob stat

Answer: D

NEW QUESTION 138
- (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 140
- (Exam Topic 2)
How often does Threat Emulation download packages by default?

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

Answer: D

NEW QUESTION 144
- (Exam Topic 2)
What is the name of the secure application for Mail/Calendar for mobile devices?

A. Capsule Workspace
B. Capsule Mail
C. Capsule VPN
D. Secure Workspace

Answer: A

NEW QUESTION 146
- (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 147
- (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 148
- (Exam Topic 2)

Which encryption algorithm is the least secured?

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

Answer: C

NEW QUESTION 150
- (Exam Topic 2)
Which command shows the current connections distributed by CoreXL FW instances?

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

Answer: A

NEW QUESTION 155
- (Exam Topic 2)
How do Capsule Connect and Capsule Workspace differ?

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

Answer: A

NEW QUESTION 158
- (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 159
- (Exam Topic 2)
The Correlation Unit performs all but the following actions:

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

Answer: C

NEW QUESTION 161
- (Exam Topic 2)
Which command shows detailed information about VPN tunnels?

A. cat $FWDIR/conf/vpn.conf
B. vpn tu tlist
C. vpn tu
D. cpview

Answer: B

NEW QUESTION 163
- (Exam Topic 2)
What command can you use to have cpinfo display all installed hotfixes?

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

Answer: B

NEW QUESTION 168
- (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 169
- (Exam Topic 2)
SmartEvent does NOT use which of the following procedures to identify events:

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

Answer: C

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

NEW QUESTION 172
- (Exam Topic 2)
From SecureXL perspective, what are the tree paths of traffic flow:

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

Answer: D

NEW QUESTION 177
- (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 182
- (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 183
- (Exam Topic 2)
What is the purpose of Priority Delta in VRRP?

A. When a box up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fail, Effective Priority = Priority – Priority Delta
D. When a box fail, Effective Priority = Priority – Priority Delta

Answer: C

Explanation:
Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP

HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP. References:

NEW QUESTION 184
- (Exam Topic 2)
What API command below creates a new host with the name “New Host” and IP address of “192.168.0.10”?

A. new host name “New Host” ip-address “192.168.0.10”
B. set host name “New Host” ip-address “192.168.0.10”
C. create host name “New Host” ip-address “192.168.0.10”
D. add host name “New Host” ip-address “192.168.0.10”

Answer: D

NEW QUESTION 186
- (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 191
- (Exam Topic 2)
Which one of the following is true about Capsule Connect?

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

Answer: A

NEW QUESTION 193
- (Exam Topic 2)
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 197
- (Exam Topic 2)
What is the difference between SSL VPN and IPSec VPN?

A. IPSec VPN does not require installation of a resilient VPN client.
B. SSL VPN requires installation of a resident VPN client.
C. SSL VPN and IPSec VPN are the same.
D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser.

Answer: D

NEW QUESTION 199
- (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 200
- (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 204
- (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 208
- (Exam Topic 2)
To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

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

Answer: C

NEW QUESTION 211
- (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 212
- (Exam Topic 2)
What is the port used for SmartConsole to connect to the Security Management Server?

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

Answer: A

NEW QUESTION 214
- (Exam Topic 2)
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

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

Answer: C

NEW QUESTION 215
- (Exam Topic 2)
The following command is used to verify the CPUSE version:

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

Answer:

A

NEW QUESTION 219
- (Exam Topic 3)
What cloud-based SandBlast Mobile application is used to register new devices and users?

A. Check Point Protect Application
B. Management Dashboard
C. Behavior Risk Engine
D. Check Point Gateway

Answer: D

NEW QUESTION 220
- (Exam Topic 3)
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

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

Answer: D

NEW QUESTION 223
- (Exam Topic 3)
Which is NOT a SmartEvent component?

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

Answer: C

NEW QUESTION 224
- (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 225
- (Exam Topic 3)
Please choose the path to monitor the compliance status of the Check Point R81.10 based management.

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

Answer: C

NEW QUESTION 230
- (Exam Topic 3)
Which file gives you a list of all security servers in use, including port number?

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

Answer: C

NEW QUESTION 234
- (Exam Topic 3)
What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 236
- (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 239
- (Exam Topic 3)
How many policy layers do Access Control policy support?

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

Answer: A

Explanation:
Two policy layers:
- Network Policy Layer
- Application Control Policy Layer

NEW QUESTION 240
- (Exam Topic 3)
You can access the ThreatCloud Repository from:

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

Answer: D

NEW QUESTION 245
- (Exam Topic 3)
What is true of the API server on R81.10?

A. By default the API-server is activated and does not have hardware requirements.
B. By default the API-server is not active and should be activated from the WebUI.
C. By default the API server is active on management and stand-alone servers with 16GB of RAM (or more).
D. By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8GB of RAM (or more).

Answer: D

NEW QUESTION 248
- (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 251
- (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 254
- (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 255
- (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 257
- (Exam Topic 3)
What command would show the API server status?

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

Answer: C

NEW QUESTION 259
- (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 261
- (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 263
- (Exam Topic 3)
Fill in the blanks. There are _____ types of software containers: _____.

A. Three; security management, Security Gateway, and endpoint security
B. Three; Security Gateway, endpoint security, and gateway management
C. Two; security management and endpoint security
D. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 265
- (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 270
- (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 275
- (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 277
- (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 281
- (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 285
- (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 289
- (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 290
- (Exam Topic 3)
Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows then as prioritized security events.

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

Answer: B

NEW QUESTION 295
- (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 297
- (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 300
- (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 304
- (Exam Topic 3)
Which blades and or features are not supported in R81?

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

Answer: A

NEW QUESTION 308
- (Exam Topic 3)
Which NAT rules are prioritized first?

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

Answer: B

NEW QUESTION 313
- (Exam Topic 3)
What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

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

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

Answer: A

NEW QUESTION 314
- (Exam Topic 3)
After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust.
B. The Security Gateway name cannot be changed in command line without re-establishing trust.
C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust.
D. The Security Management Server IP-address cannot be changed without re-establishing the trust.

Answer: A

NEW QUESTION 316
- (Exam Topic 3)
The SmartEvent R81 Web application for real-time event monitoring is called:

A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView

Answer: B

NEW QUESTION 317
- (Exam Topic 3)
Which Check Point feature enables application scanning and the detection?

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

Answer: B

NEW QUESTION 322
- (Exam Topic 3)
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

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

Answer: D

NEW QUESTION 326
- (Exam Topic 3)
Which of the following is NOT a VPN routing option available in a star community?

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

Answer: AD

NEW QUESTION 327
- (Exam Topic 3)
What is the command to show SecureXL status?

A. fwaccel status
B. fwaccel stats -m
C. fwaccel -s
D. fwaccel stat

Answer: D

Explanation:
To check overall SecureXL status: [Expert@HostName]# fwaccel stat References:

NEW QUESTION 328

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

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

Answer: C

NEW QUESTION 330
- (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 335
- (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 337
- (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 341
- (Exam Topic 3)
SmartEvent provides a convenient way to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands. They appear only on cells that refer to IP addresses because the IP address of the active cell is used as the destination of the command when run. The default commands are:

A. ping, traceroute, netstat, and route
B. ping, nslookup, Telnet, and route
C. ping, whois, nslookup, and Telnet
D. ping, traceroute, netstat, and nslookup

Answer: C

NEW QUESTION 346
- (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 348
- (Exam Topic 3)
Ken wants to obtain a configuration lock from other administrator on R81 Security Management Server. He can do this via WebUI or via CLI.
Which command should he use in CLI? (Choose the correct answer.)

A. remove database lock

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

Answer: D

NEW QUESTION 351
- (Exam Topic 3)
Which path below is available only when CoreXL is enabled?

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

Answer: C

NEW QUESTION 356
- (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 360
- (Exam Topic 3)
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 361
- (Exam Topic 3)
What must you do first if "fwm sic_reset" could not be completed?

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

Answer: D

NEW QUESTION 365
- (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 368
- (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 370

- (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 372
- (Exam Topic 3)
With SecureXL enabled, accelerated packets will pass through the following:

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

Answer: C

NEW QUESTION 375
- (Exam Topic 4)
Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

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

Answer: B

NEW QUESTION 377
- (Exam Topic 4)
Firewall polices must be configured to accept VRRP packets on the GAiA platform if it Firewall software. The Multicast destination assigned by the internet Assigned Number Authority (IANA) for VRRP is:

A. 224.0.0.18
B. 224 00 5
C. 224.0.0.102
D. 224.0.0.22

Answer: A

NEW QUESTION 379
- (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 382
- (Exam Topic 4)
What is the default size of NAT table fwx_alloc?

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

Answer: C

NEW QUESTION 385
- (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 387
- (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 391
- (Exam Topic 4)
Installations and upgrades with CPUSE require that the CPUSE agent is up-to-date. Usually the latest build is downloaded automatically. How can you verify the CPUSE agent build?

A. In WebUI Status and Actions page or by running the following command in CLISH: show installer status build
B. In WebUI Status and Actions page or by running the following command in CLISH: show installer status version
C. In the Management Server or Gateway object in SmartConsole or by running the following command in CLISH: show installer status build
D. In the Management Server or Gateway object in SmartConsole or by running the following command in CLISH: show installer agent

Answer: A

NEW QUESTION 396
- (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 401
- (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 404
- (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 405
- (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 407
- (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 410
- (Exam Topic 4)
What are the modes of SandBlast Threat Emulation deployment?

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

Answer: D

NEW QUESTION 413
- (Exam Topic 4)
What are the services used for Cluster Synchronization?

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

Answer: C

NEW QUESTION 415
- (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 418
- (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 421
- (Exam Topic 4)
After having saved the Cllsh Configuration with the "save configuration config.txt* command, where can you find the config.txt file?

A. You will find it in the home directory of your usef account (e.
B. /home/admirV)
C. You can locate the file via SmartConsole > Command Line.
D. You have to launch the WebUl and go to "Config" -> "Export Conflg File" and specifly the destination directory of your local tile system
E. You cannot locate the file in the file system sine© Clish does not have any access to the bash fie system

Answer: B

NEW QUESTION 425
- (Exam Topic 4)
How long may verification of one file take for Sandblast Threat Emulation?

A. up to 1 minutes
B. within seconds cleaned file will be provided

C. up to 5 minutes
D. up to 3 minutes

Answer: B

NEW QUESTION 429
- (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 433
- (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 437
- (Exam Topic 4)
Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.

A. Better understand the behavior of the Access Control Policy
B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base
C. Automatically rearrange Access Control Policy based on Hit Count Analysis
D. Analyze a Rule Base - You can delete rules that have no matching connections

Answer: C

NEW QUESTION 440
- (Exam Topic 4)
Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

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

Answer: A

NEW QUESTION 444
- (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 445
- (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 446
- (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 447
- (Exam Topic 4)
John detected high load on sync interface. Which is most recommended solution?

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

Answer: A

NEW QUESTION 448
- (Exam Topic 4)
What is required for a site-to-site VPN tunnel that does not use certificates?

A. Pre-Shared Secret
B. RSA Token
C. Unique Passwords
D. SecurelD

Answer: A

NEW QUESTION 449
- (Exam Topic 4)
GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

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

Answer: A

NEW QUESTION 450
- (Exam Topic 4)
Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?

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

Answer: B

NEW QUESTION 454
- (Exam Topic 4)
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

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

Answer: B

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

NEW QUESTION 456
- (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 461
- (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 465
- (Exam Topic 4)
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

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

Answer: B

NEW QUESTION 466
- (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 470
- (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 474
- (Exam Topic 4)
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

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

Answer: B

NEW QUESTION 477
- (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 480

- (Exam Topic 4)
Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 485
- (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 486
- (Exam Topic 4)
Which Correction mechanisms are available with ClusterXL under R81.10?

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

Answer: C

NEW QUESTION 489
- (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 493
- (Exam Topic 4)
The Compliance Blade allows you to search for text strings in many windows and panes, to search for a value in a field, what would your syntax be?

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

Answer: A

NEW QUESTION 497
- (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 501
- (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 505
- (Exam Topic 4)
The WebUI offers several methods for downloading hotfixes via CPUSE except:

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

Answer: B

NEW QUESTION 509
- (Exam Topic 4)
In the R81 SmartConsole, on which tab are Permissions and Administrators defined?

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

Answer: C

NEW QUESTION 513
- (Exam Topic 4)
If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

A. Nothing - the proxy ARP is automatically handled in the R81 version
B. Add the proxy ARP configurations in a file called /etc/conf/local.arp
C. Add the proxy ARP configurations in a file called $FWDIR/conf/local.arp
D. Add the proxy ARP configurations in a file called $CPDIR/conf/local.arp

Answer: D

NEW QUESTION 515
- (Exam Topic 4)
In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

A. Limit
B. Resource
C. Custom Application / Site
D. Network Object

Answer: B

NEW QUESTION 516
- (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 517
- (Exam Topic 4)
What is the command used to activated Multi-Version Cluster mode?

A. set cluster member mvc on in Clish

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

Answer: A

NEW QUESTION 519
- (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 524
- (Exam Topic 4)
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

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

Answer: C

NEW QUESTION 527
- (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 529
- (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 532
- (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 536
- (Exam Topic 4)
When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

A. Network, and defining your Class A space
B. Topology, and you are defining the Internal network
C. Internal addresses you are defining the gateways
D. Internal network(s) you are defining your networks

Answer: D

NEW QUESTION 538
- (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 543
- (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 546
- (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 547
- (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 551
- (Exam Topic 4)
Besides fw monitor, what is another command that can be used to capture packets?

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

Answer: C

NEW QUESTION 552
- (Exam Topic 4)
To find records in the logs that shows log records from the Application & URL Filtering Software Blade where traffic was dropped, what would be the query syntax?

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

Answer: D

NEW QUESTION 553

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

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

Answer: A

NEW QUESTION 555
- (Exam Topic 4)
According to the policy installation flow the transfer state (CPTA) is responsible for the code generated by the FWM. On the Security Gateway side a process receives them and first stores them Into a temporary directory. Which process is true for receiving these Tiles;

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

Answer: A

NEW QUESTION 558
- (Exam Topic 4)
Which software blade does NOT accompany the Threat Prevention policy?

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

Answer: D

NEW QUESTION 560
- (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 561
- (Exam Topic 4)
What are the available options for downloading Check Point hotfixes in Gala WebUI (CPUSE)?

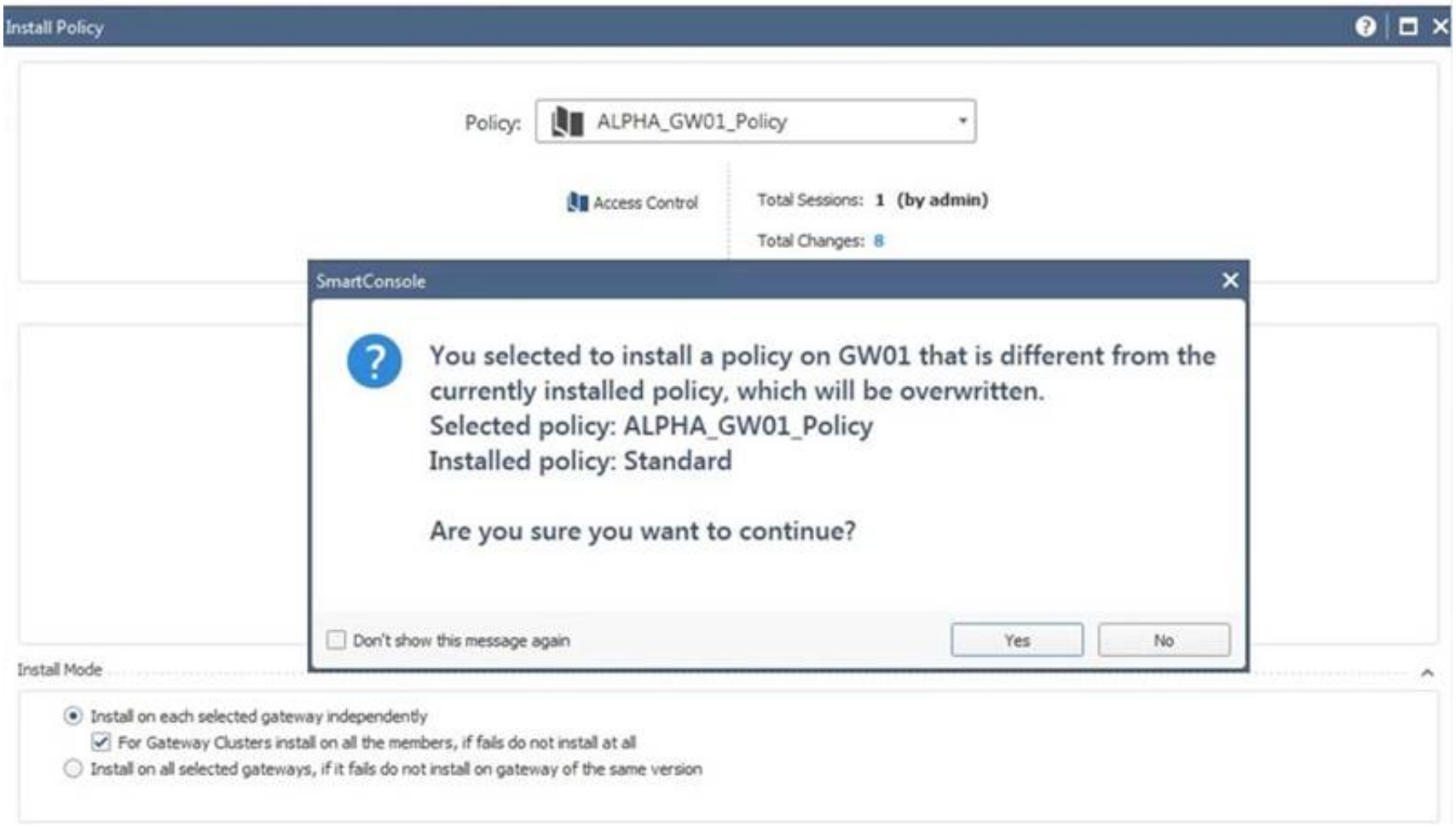
A. Manually, Scheduled, Automatic
B. Manually, Automatic, Disabled
C. Manually, Scheduled, Disabled
D. Manually, Scheduled, Enabled

Answer: A

Explanation:

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

NEW QUESTION 566
- (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 571
- (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 576
- (Exam Topic 4)
An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?

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

Answer: D

NEW QUESTION 577
- (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

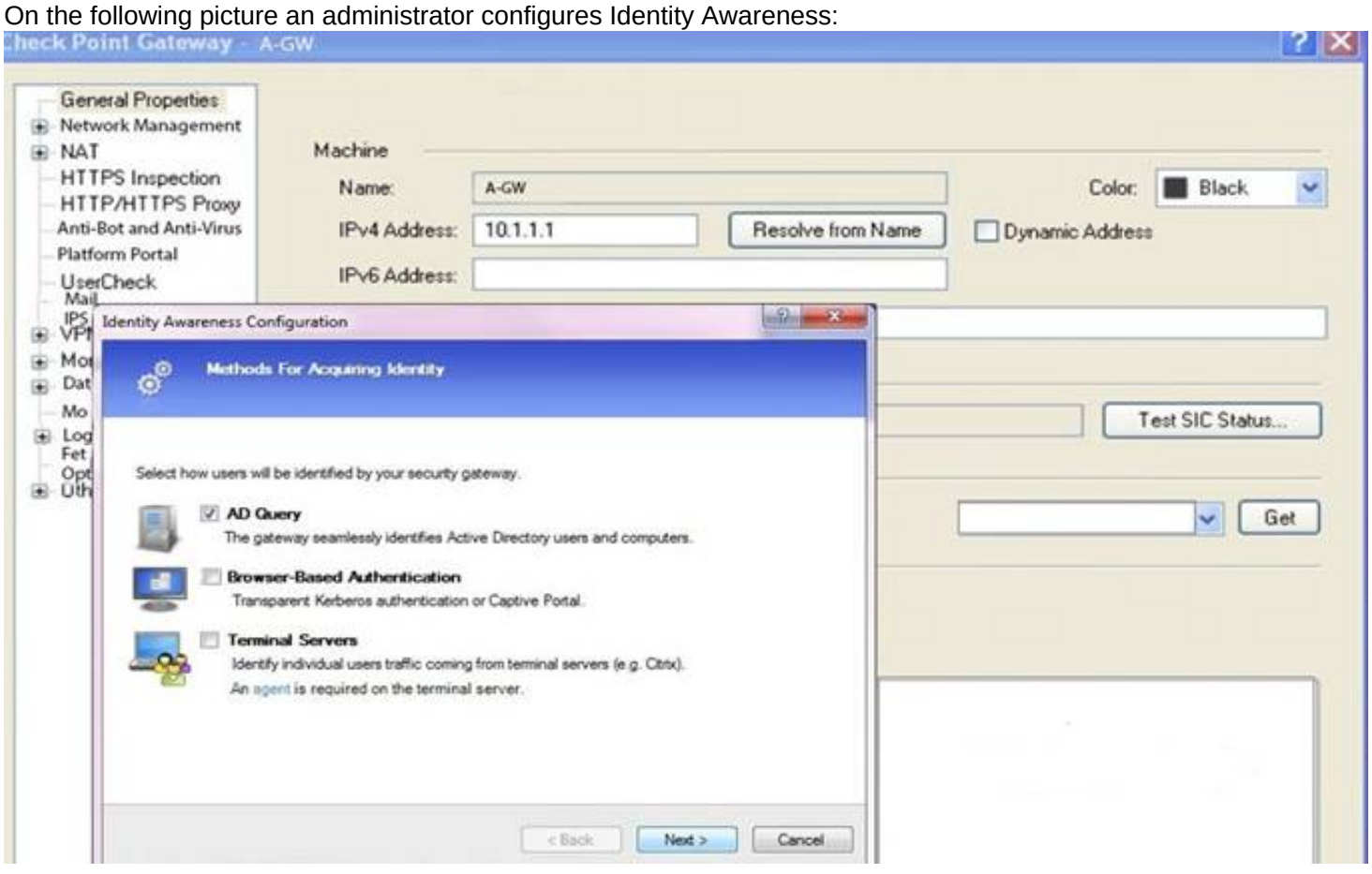
NEW QUESTION 579
- (Exam Topic 4)
UserCheck objects in the Application Control and URL Filtering rules allow the gateway to communicate with the users. Which action is not supported in UserCheck objects?

A. Ask
B. Drop

C. Inform
D. Reject

Answer: D

NEW QUESTION 584
- (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 585
- (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 586
- (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 591
- (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 593
- (Exam Topic 4)
The log server sends what to the Correlation Unit?

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

Answer: C

NEW QUESTION 597
- (Exam Topic 4)
IF the first packet of an UDP session is rejected by a rule definition from within a security policy (not including the clean up rule), what message is sent back through the kernel?

A. Nothing
B. TCP FIN
C. TCP RST
D. ICMP unreachable

Answer: A

NEW QUESTION 600
- (Exam Topic 4)
You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

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

Answer: A

NEW QUESTION 602
- (Exam Topic 4)
SmartConsole R81 x requires the following ports to be open for SmartEvent.

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

Answer: D

NEW QUESTION 603
- (Exam Topic 4)
At what point is the Internal Certificate Authority (ICA) created?

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

Answer: B

NEW QUESTION 604
- (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 607
- (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 611
- (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 613
- (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 618
- (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 622
- (Exam Topic 4)
What are the two modes for SNX (SSL Network Extender)?

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

Answer: A

NEW QUESTION 627
- (Exam Topic 4)
What command is used to manually failover a cluster during a zero downtime upgrade?

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

Answer: C

NEW QUESTION 628
- (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 630
- (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 631
- (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 634
- (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 636
- (Exam Topic 4)
Fill in the blanks: Gaia can be configured using the _____ or _____.

A. GaiaUI; command line interface
B. WebUI; Gaia Interface
C. Command line interface; WebUI
D. Gaia Interface; GaiaUI

Answer: C

NEW QUESTION 641
- (Exam Topic 4)
Which is the command to identify the NIC dnver before considering about the employment of the Multi-Queue feature?

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

Answer: A

NEW QUESTION 642
- (Exam Topic 4)
What are the three SecureXL Templates available in R81.10?

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

Answer: B

NEW QUESTION 646
- (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 648
.....

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