Exam Questions 156-315.81

Check Point Certified Security Expert R81

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

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

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

Answer: B

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

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

Answer: D

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

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

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
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 5
- (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 6
- (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 7
- (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 8
- (Exam Topic 1)
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

A. Secure Internal Communication (SIC)
B. Restart Daemons if they fail
C. Transfers messages between Firewall processes
D. Pulls application monitoring status

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
The 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 10
- (Exam Topic 1)
The Security Gateway is installed on GAIA R81. The default port for the Web User Interface is ______.

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

Answer: D

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

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

Answer: C

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

NEW QUESTION 12
- (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 14
- (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 17
- (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 18
- (Exam Topic 1)
Advanced Security Checkups can be easily conducted within:

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

Answer: A

NEW QUESTION 19
- (Exam Topic 1)
During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

A. Host having a Critical event found by Threat Emulation
B. Host having a Critical event found by IPS
C. Host having a Critical event found by Antivirus
D. Host having a Critical event found by Anti-Bot

Answer: D

NEW QUESTION 24
- (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 25
- (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 28
- (Exam Topic 1)
The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

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

Answer: A

NEW QUESTION 33
- (Exam Topic 1)
To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:

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

Answer: D

NEW QUESTION 35
- (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 37
- (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 l
B. Little o
C. Little i
D. Big O

Answer: A

NEW QUESTION 42
- (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 45
- (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 50
- (Exam Topic 1)
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

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

Answer: D

NEW QUESTION 53
- (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 56
- (Exam Topic 1)
You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup
B. import backup
C. cp_merge
D. migrate import

Answer: D

NEW QUESTION 57
- (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 59
- (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 63
- (Exam Topic 2)
Which GUI client is supported in R81?

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

Answer: C

NEW QUESTION 65
- (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 70
- (Exam Topic 2)
What is the purpose of a SmartEvent Correlation Unit?

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

Answer: C

NEW QUESTION 71

- (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 75
- (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 77
- (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 79
- (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 80
- (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 85
- (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 88
- (Exam Topic 2)

When gathering information about a gateway using CPINFO, what information is included or excluded when using the “-x” parameter?

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

Answer: B

NEW QUESTION 89
- (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 92
- (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 97
- (Exam Topic 2)
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

A. mgmt_cli add-host “Server_1” ip_address “10.15.123.10” --format txt
B. mgmt_cli add host name “Server_1” ip-address “10.15.123.10” --format json
C. mgmt_cli add object-host “Server_1” ip-address “10.15.123.10” --format json
D. mgmt._cli add object “Server-1” ip-address “10.15.123.10” --format json

Answer: B

Explanation:
Example:
mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json
• "--format json" is optional. By default the output is presented in plain text.

NEW QUESTION 99
- (Exam Topic 2)
What is the most recommended way to install patches and hotfixes?

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

Answer: A

NEW QUESTION 102
- (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 107
- (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 112
- (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 116
- (Exam Topic 2)
What is considered Hybrid Emulation Mode?

A. Manual configuration of file types on emulation location.
B. Load sharing of emulation between an on premise appliance and the cloud.
C. Load sharing between OS behavior and CPU Level emulation.
D. High availability between the local SandBlast appliance and the cloud.

Answer: B

NEW QUESTION 121
- (Exam Topic 2)
Which of the following links will take you to the SmartView web application?

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

Answer: B

NEW QUESTION 122
- (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 123
- (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 126
- (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 130
- (Exam Topic 2)
SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

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

Answer: A

NEW QUESTION 133
- (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 135
- (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 140
- (Exam Topic 2)
To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

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

Answer: B

NEW QUESTION 142
- (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 144
- (Exam Topic 3)
On what port does the CPM process run?

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

Answer: D

NEW QUESTION 147
- (Exam Topic 3)
Joey wants to upgrade from R75.40 to R81 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this. What is one of the requirements for his success?

A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine
B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
C. Size of the $FWDIR/log folder of the target machine must be at least 30% of the size of the$FWDIR/log directory on the source machine
D. Size of the /var/log folder of the target machine must be at least 25GB or more

Answer: B

NEW QUESTION 151
- (Exam Topic 3)
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 154
- (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 156
- (Exam Topic 3)
What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 160
- (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 164
- (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 168
- (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 173
- (Exam Topic 3)
You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.

What must you do to get SIC to work?

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

Answer: C

NEW QUESTION 174
- (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 176
- (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 177
- (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 180
- (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 184
- (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 186

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

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

Answer: C

NEW QUESTION 195
- (Exam Topic 3)
Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is ______ .

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

Answer: D

NEW QUESTION 198
- (Exam Topic 3)
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 201
- (Exam Topic 3)
SandBlast agent extends 0 day prevention to what part of the network?

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

Answer: A

NEW QUESTION 203
- (Exam Topic 3)
Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _______ consolidate billions of logs and shows then as prioritized security events.

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

Answer: B

NEW QUESTION 207
- (Exam Topic 3)
What 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 210
- (Exam Topic 3)
What is UserCheck?

A. Messaging tool used to verify a user’s credentials.
B. Communication tool used to inform a user about a website or application they are trying to access.
C. Administrator tool used to monitor users on their network.
D. Communication tool used to notify an administrator when a new user is created.

Answer: B

NEW QUESTION 213
- (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 216
- (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 221
- (Exam Topic 3)
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _______.

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

Answer: B

NEW QUESTION 223
- (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 227
- (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 232
- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

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

Answer: D

NEW QUESTION 233
- (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 238
- (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 239
- (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 244
- (Exam Topic 3)
Vanessa is a Firewall administrator. She wants to test a backup of her company’s production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment.
Which details she need to fill in System Restore window before she can click OK button and test the backup?

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

Answer: C

NEW QUESTION 246
- (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 250
- (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 251
- (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 252
- (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 255
- (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 258
- (Exam Topic 4)
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsive, which if these steps should NOT be performed:

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

Answer: A

NEW QUESTION 259
- (Exam Topic 4)
After finishing installation admin John likes to use top command in expert mode. John has to set the
expert-password and was able to use top command. A week later John has to use the top command again, He detected that the expert password is no longer valid. What is the most probable reason for this behavior?

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

Answer: D

NEW QUESTION 263
- (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 267
- (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 268
- (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 272
- (Exam Topic 4)
Which feature is NOT provided by all Check Point Mobile Access solutions?

A. Support for IPv6
B. Granular access control
C. Strong user authentication
D. Secure connectivity

Answer: A

Explanation:
Types of Solutions
All of Check Point's Remote Access solutions provide:

NEW QUESTION 277
- (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 281
- (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 282
- (Exam Topic 4)
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

Answer: B

NEW QUESTION 284

- (Exam Topic 4)
What command is used to manually failover a Multi-Version Cluster during the upgrade?

A. clusterXL_admin down in Expert Mode
B. clusterXL_admin down in Clish
C. set cluster member state down in Clish
D. set cluster down in Expert Mode

Answer: B

NEW QUESTION 287
- (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 290
- (Exam Topic 4)
What traffic does the Anti-bot feature block?

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

Answer: A

NEW QUESTION 292
- (Exam Topic 4)
Which command will reset the kernel debug options to default settings?

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

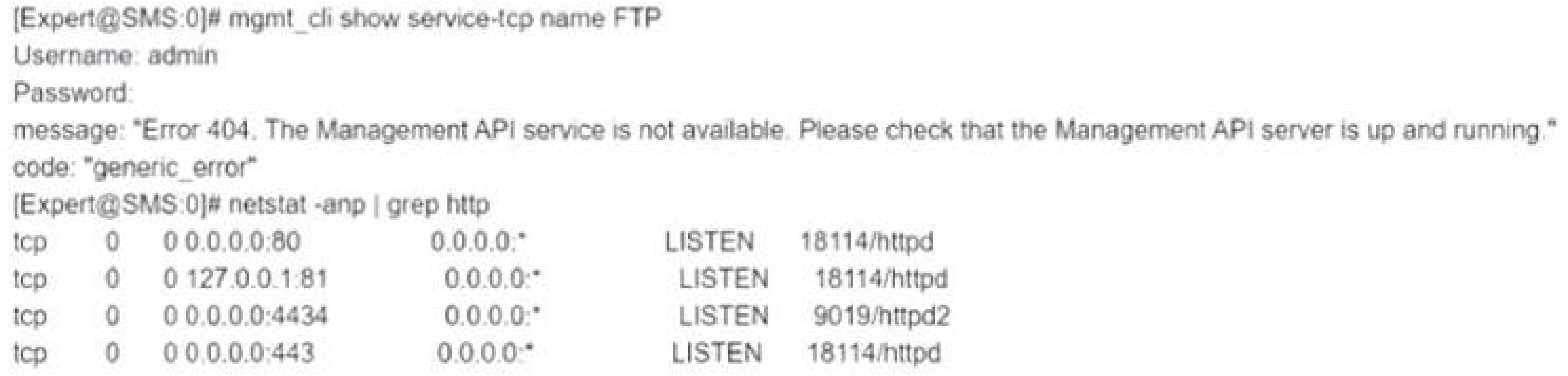
Answer: C

NEW QUESTION 294
- (Exam Topic 4)
What solution is Multi-queue intended to provide?

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

Answer: C

NEW QUESTION 296
- (Exam Topic 4)
The admin is connected via ssh lo the management server. He wants to run a mgmt_dl command but got a Error 404 message. To check the listening ports on the management he runs netstat with the results shown below. What can be the cause for the issue?



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

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

F. The API is not running, the services shown by netstat are the gaia service
G. To start the API run 'api start'

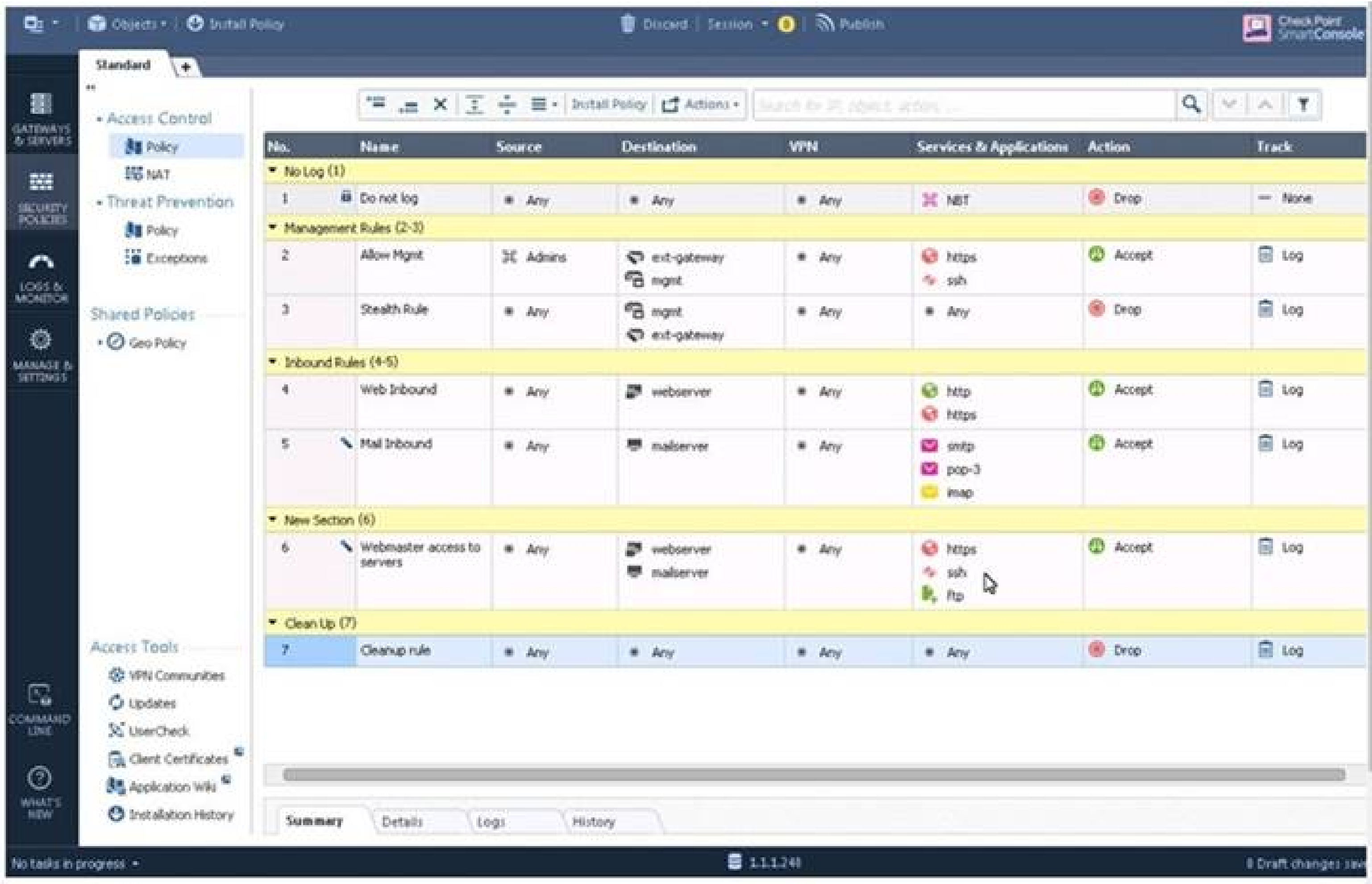
Answer: A

NEW QUESTION 300
- (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 303
- (Exam Topic 4)



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NBT	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept	Log
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop	Log
Inbound Rules (4-5)							
4	Web Inbound	Any	webserver	Any	http https	Accept	Log
5	Mail Inbound	Any	mailserver	Any	smtp pop-3 imap	Accept	Log
New Section (6)							
6	Webmaster access to servers	Any	webserver mailserver	Any	https ssh ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

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 305
- (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 307
- (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 312
- (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 316
- (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 318
- (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 321
- (Exam Topic 4)
When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

A. Syslog
B. SNMPTrap
C. Block Source
D. Mail

Answer: B

NEW QUESTION 324
- (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 328
- (Exam Topic 4)
Which member of a high-availability cluster should be upgraded first in a Zero downtime upgrade?

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

Answer: A

NEW QUESTION 332
- (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 335
- (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 339
- (Exam Topic 4)
What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

A. Idle <20%
B. USR <20%
C. SYS <20%
D. Wait <20%

Answer: A

NEW QUESTION 342
- (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 346
- (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 348
- (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 350
- (Exam Topic 4)
DLP and Geo Policy are examples of what type of Policy?

A. Standard Policies
B. Shared Policies
C. Inspection Policies
D. Unified Policies

Answer: B

NEW QUESTION 351

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

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

Answer: D

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

NEW QUESTION 356
- (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 359
- (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 363
- (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 368
- (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 372
- (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 375
- (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

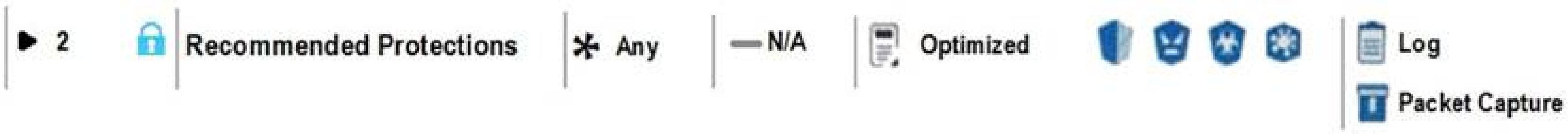
NEW QUESTION 378
- (Exam Topic 4)
Which of the following is a task of the CPD process?

A. Invoke and monitor critical processes and attempts to restart them if they fail
B. Transfers messages between Firewall processes
C. Log forwarding
D. Responsible for processing most traffic on a security gateway

Answer: B

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

NEW QUESTION 382
- (Exam Topic 4)
View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



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

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

Answer: B

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

NEW QUESTION 383
- (Exam Topic 4)
What component of Management is used tor indexing?

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

Answer: D

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

NEW QUESTION 388
- (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 389
- (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 390
- (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 391
- (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 392
- (Exam Topic 4)
How can you switch the active log file?

A. Run fw logswitch on the gateway
B. Run fwm logswitch on the Management Server
C. Run fwm logswitch on the gateway
D. Run fw logswitch on the Management Server

Answer: D

NEW QUESTION 396
- (Exam Topic 4)
Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:

A. ReverseCLIProxy
B. ReverseProxyCLI
C. ReverseProxy
D. ProxyReverseCLI

Answer: C

NEW QUESTION 398
- (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 399
- (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 403

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

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

Answer: A

NEW QUESTION 405
- (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 407
- (Exam Topic 4)
What mechanism can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources?

A. The corresponding feature is new to R81.10 and is called "Management Data Plane Separation"
B. The corresponding feature is called "Dynamic Dispatching"
C. There is a feature for ensuring stable connectivity to the management server and is done via Priority Queuing.
D. The corresponding feature is called "Dynamic Split"

Answer: A

NEW QUESTION 411
- (Exam Topic 4)
What is the correct description for the Dynamic Balancing / Split feature?

A. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current loa
B. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
C. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND'
D. The interface must support Multi-Queu
E. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
F. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND'
G. The interface must support Multi-Queu
H. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
I. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current loa
J. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

Answer: D

NEW QUESTION 415
- (Exam Topic 4)
Which command is used to add users to or from existing roles?

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

Answer: A

NEW QUESTION 418
- (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 423
- (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 428
- (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 433
- (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 436
- (Exam Topic 4)
Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

A. Security Gateway Clusters in Load Sharing mode
B. Dedicated Log Server
C. Dedicated SmartEvent Server
D. Security Gateways/Clusters in ClusterXL HA new mode

Answer: D

NEW QUESTION 437
- (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 438
- (Exam Topic 4)
Fill in the blank: _______ information is included in “Full Log” tracking option, but is not included in “Log” tracking option?

A. Destination port
B. Data type
C. File attributes
D. Application

Answer: B

NEW QUESTION 439
- (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 443
- (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 444
- (Exam Topic 4)
CoreXL is NOT supported when one of the following features is enabled: (Choose three)

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

Answer: ACD

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

- Check Point QoS (Quality of Service)
- Route-based VPN
- IPv6 on IPSO
- Overlapping NAT

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

NEW QUESTION 447
- (Exam Topic 4)
By default, which port does the WebUI listen on?

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

Answer: C

NEW QUESTION 452
- (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 455
......