



CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

NEW QUESTION 1

- (Exam Topic 1)

Which is NOT an example of a Check Point API?

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

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

Which of these statements describes the Check Point ThreatCloud?

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

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

How can SmartView application accessed?

- A. `http://<Security Management IP Address>/smartview`
- B. `http://<Security Management IP Address>:4434/smartview/`
- C. `https://<Security Management IP Address>/smartview/`
- D. `https://<Security Management host name>:4434/smartview/`

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

fwssd is a child process of which of the following Check Point daemons?

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

Answer: A

NEW QUESTION 5

- (Exam Topic 1)

You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) _____ or _____ action for the file types.

- A. Inspect/Bypass
- B. Inspect/Prevent
- C. Prevent/Bypass
- D. Detect/Bypass

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

Fill in the blank: The R81 utility fw monitor is used to troubleshoot .

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

Answer: C

Explanation:

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

NEW QUESTION 8

- (Exam Topic 1)

You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

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

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

Which TCP-port does CPM process listen to?

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

Answer: D

NEW QUESTION 10

- (Exam Topic 1)

Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

- A. Check Point Remote User
- B. Check Point Capsule Workspace
- C. Check Point Mobile Web Portal
- D. Check Point Capsule Remote

Answer: C

NEW QUESTION 15

- (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 16

- (Exam Topic 1)

What happen when IPS profile is set in Detect Only Mode for troubleshooting?

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

Answer: C

Explanation:

It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic.

During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION 19

- (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 20

- (Exam Topic 1)

Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

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

Answer: D

NEW QUESTION 22

- (Exam Topic 1)

Which command would disable a Cluster Member permanently?

- A. clusterXL_admin down
- B. cphaprob_admin down
- C. clusterXL_admin down-p
- D. set clusterXL down-p

Answer: C

NEW QUESTION 24

- (Exam Topic 1)

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated management console. It empowers the migration from legacy Client-side logic to Server-side logic. The cpm process:

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

Answer: C

NEW QUESTION 28

- (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 33

- (Exam Topic 1)

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Symmetric routing
- B. Failovers
- C. Asymmetric routing
- D. Anti-Spoofing

Answer: C

NEW QUESTION 36

- (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 37

- (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 38

- (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 40

- (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 42

- (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 46

- (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 51

- (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 55

- (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 56

- (Exam Topic 2)

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

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

Answer: C

NEW QUESTION 57

- (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 58

- (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 62

- (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 65

- (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 68

- (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 71

- (Exam Topic 2)

Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 75

- (Exam Topic 2)

What processes does CPM control?

- A. Object-Store, Database changes, CPM Process and web-services
- B. web-services, CPML process, DLEserver, CPM process
- C. DLEServer, Object-Store, CP Process and database changes
- D. web_services, dle_server and object_Store

Answer: D

NEW QUESTION 79

- (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 82

- (Exam Topic 2)

To add a file to the Threat Prevention Whitelist, what two items are needed?

- A. File name and Gateway
- B. Object Name and MD5 signature
- C. MD5 signature and Gateway
- D. IP address of Management Server and Gateway

Answer: B

NEW QUESTION 86

- (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 91

- (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 begin 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 96

- (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 101

- (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 102

- (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 104

- (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 105

- (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 106

- (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 108

- (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 110

- (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 113

- (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 117

- (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 118

- (Exam Topic 3)

What statement best describes the Proxy ARP feature for Manual NAT in R81.10?

- A. Automatic proxy ARP configuration can be enabled
- B. Translate Destination on Client Side should be configured
- C. fw ctl proxy should be configured
- D. local.arp file must always be configured

Answer: D

NEW QUESTION 121

- (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 125

- (Exam Topic 3)

What is the Implicit Clean-up Rule?

- A. A setting is defined in the Global Properties for all policies.
- B. A setting that is configured per Policy Layer.
- C. Another name for the Clean-up Rule.
- D. Automatically created when the Clean-up Rule is defined.

Answer: C

NEW QUESTION 128

- (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 CoreXI FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type

Answer: B

NEW QUESTION 130

- (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 132

- (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 134

- (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 137

- (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 140

- (Exam Topic 3)

Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

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

Answer: B

NEW QUESTION 143

- (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 145

- (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 149

- (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 154

- (Exam Topic 3)

Which of the following commands shows the status of processes?

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

Answer: D

NEW QUESTION 157

- (Exam Topic 3)

After the initial installation on Check Point appliance, you notice that the Management-interface and default gateway are incorrect.

Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
- B. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
- D. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 159

- (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 160

- (Exam Topic 3)

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT
- B. IP pool NAT, static NAT, hide NAT
- C. Static NAT, automatic NAT, hide NAT
- D. Static NAT, hide NAT, IP pool NAT

Answer: A

NEW QUESTION 164

- (Exam Topic 3)

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated.

What is the most likely reason that the traffic is not accelerated?

- A. There is a virus found
- B. Traffic is still allowed but not accelerated.
- C. The connection required a Security server.

- D. Acceleration is not enabled.
- E. The traffic is originating from the gateway itself.

Answer: B

NEW QUESTION 166

- (Exam Topic 3)

What is the responsibility of SOLR process on R81.10 management server?

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

Answer: B

NEW QUESTION 171

- (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 173

- (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 177

- (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 181

- (Exam Topic 4)

What are the minimum open server hardware requirements for a Security Management Server/Standalone in R81?

- A. 2 CPU cores, 4GB of RAM and 15GB of disk space
- B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
- C. 4 CPU cores, 8GB of RAM and 500GB of disk space
- D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Answer: C

NEW QUESTION 182

- (Exam Topic 4)

Kurt is planning to upgrade his Security Management Server to R81.X. What is the lowest supported version of the Security Management he can upgrade from?

- A. R76 Splat
- B. R77.X Gaia
- C. R75 Splat
- D. R75 Gaia

Answer: D

NEW QUESTION 187

- (Exam Topic 4)

What are types of Check Point APIs available currently as part of R81.10 code?

- A. Security Gateway API Management API, Threat Prevention API and Identity Awareness Web Services API
- B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
- C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
- D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 188

- (Exam Topic 4)

What a valid SecureXL paths in R81.10?

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

Answer: D

NEW QUESTION 190

- (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 192

- (Exam Topic 4)

Which of the following is NOT a valid type of SecureXL template?

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

Answer: B

NEW QUESTION 195

- (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 logged 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 199

- (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 204

- (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 205

- (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 209

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 211

- (Exam Topic 4)

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

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

Answer: D

Explanation:

Identity Awareness gets identities from these acquisition sources:

NEW QUESTION 214

- (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 218

- (Exam Topic 4)

The admin is connected via ssh lo the management server. He wants to run a mgmt_cli 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 0.127.0.0:181      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 lthe 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_cli 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 222

- (Exam Topic 4)

Can Check Point and Third-party Gateways establish a certificate-based Site-to-Site VPN tunnel?

- A. Yes, but they need to have a mutually trusted certificate authority
- B. Yes, but they have to have a pre-shared secret key
- C. No, they cannot share certificate authorities
- D. No, Certificate based VPNs are only possible between Check Point devices

Answer: A

NEW QUESTION 227

- (Exam Topic 4)

You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?

- A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH
- B. ifconfig eth1 hw 11:11:11:11:11:11; expert
- C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
- D. ethtool -i eth2 mac 11:11:11:11:11:11; expert

Answer: A

NEW QUESTION 231

- (Exam Topic 4)

What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?

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

Answer: B

NEW QUESTION 234

- (Exam Topic 4)

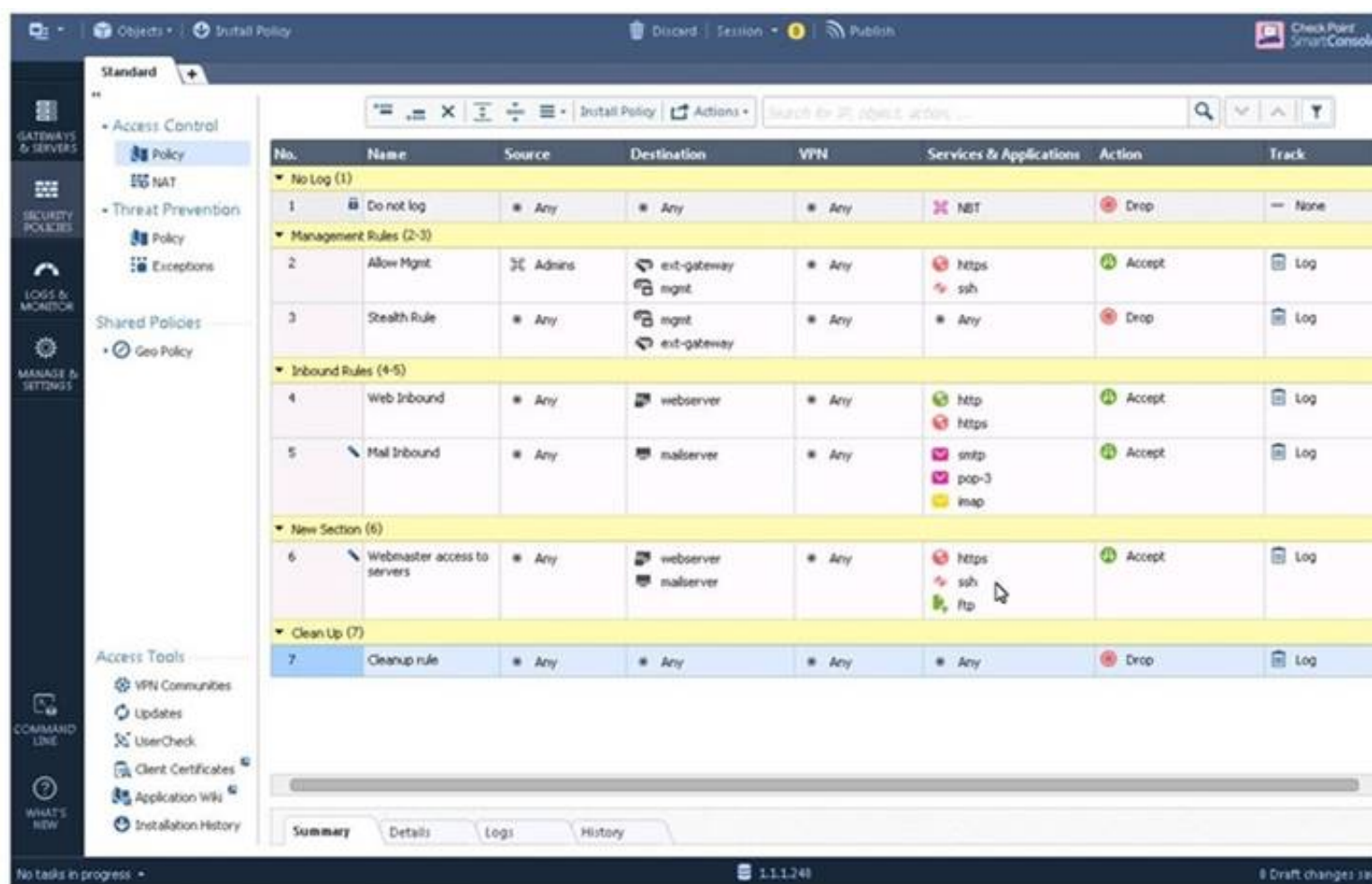
How many versions, besides the destination version, are supported in a Multi-Version Cluster Upgrade?

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

Answer: B

NEW QUESTION 236

- (Exam Topic 4)



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NET	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 240

- (Exam Topic 4)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 243

- (Exam Topic 4)

What is the base level encryption key used by Capsule Docs?

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

Answer: A

NEW QUESTION 248

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 251

- (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 253

- (Exam Topic 4)

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

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

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

Answer: C

NEW QUESTION 258

- (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 261

- (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 266

- (Exam Topic 4)

What is the correct order of the default “fw monitor” inspection points?

- A. i, l, o, O
 B. 1, 2, 3, 4
 C. i, o, l, O
 D. l, i, O, o

Answer: C

NEW QUESTION 271

- (Exam Topic 4)

Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

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

Answer: D

NEW QUESTION 274

- (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 278

- (Exam Topic 4)

What Is the difference between Updatable Objects and Dynamic Objects

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

Answer: B

NEW QUESTION 279

- (Exam Topic 4)

Joey want to configure NTP on R81 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

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

Answer: A

NEW QUESTION 283

- (Exam Topic 4)

How is communication between different Check Point components secured in R81? As with all questions, select the BEST answer.

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

Answer: B

NEW QUESTION 286

- (Exam Topic 4)

Which options are given on features, when editing a Role on Gaia Platform?

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

Answer: B

NEW QUESTION 290

- (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 294

- (Exam Topic 4)

The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?

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

Answer: C

NEW QUESTION 299

- (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 304

- (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 308

- (Exam Topic 4)

You want to gather data and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

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

Answer: B

Explanation:

SandBlast Mobile Protect is a lightweight app for iOS and Android™ that gathers data and helps analyze threats to devices in your environment.
<https://www.checkpoint.com/downloads/products/how-sandblast-mobile-works-solution-brief.pdf>

NEW QUESTION 313

- (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 314

- (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 318

- (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 322

- (Exam Topic 4)

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

Answer: D

NEW QUESTION 324

- (Exam Topic 4)

While using the Gaia CLI. what is the correct command to publish changes to the management server?

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

Answer: B

NEW QUESTION 325

- (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 327

- (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 332

- (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 337

- (Exam Topic 4)

Which of the following is NOT an attribute of packet acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. VLAN Tag

Answer: D

NEW QUESTION 340

- (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-Queue
- 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-Queue
- 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 344

- (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 345

- (Exam Topic 4)

What are not possible commands to acquire the lock in order to make changes in Clish or Web GUI?

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

Answer: C

NEW QUESTION 349

- (Exam Topic 4)

Check Point ClusterXL Active/Active deployment is used when:

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

Answer: D

NEW QUESTION 354

- (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 356

- (Exam Topic 4)

Which two Cluster Solutions are available under R81.10?

- A. ClusterXL and NSRP
- B. VRRP and HSRP
- C. VRRP and IP Clustering
- D. ClusterXL and VRitP

Answer: D

NEW QUESTION 357

- (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 362

- (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 367

- (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 372

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

156-315.81 Practice Exam Features:

- * 156-315.81 Questions and Answers Updated Frequently
- * 156-315.81 Practice Questions Verified by Expert Senior Certified Staff
- * 156-315.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-315.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-315.81 Practice Test Here](#)