

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)

Check Point Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____.

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

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

Which command is used to set the CCP protocol to Multicast?

- A. cphaprob set_ccp multicast
- B. cphaconf set_ccp multicast
- C. cphaconf set_ccp no_broadcast
- D. cphaprob set_ccp no_broadcast

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

Which command can you use to enable or disable multi-queue per interface?

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

Answer: A

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

What is the least amount of CPU cores required to enable CoreXL?

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

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

Fill in the blank: The R81 feature _____ permits blocking specific IP addresses for a specified time period.

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

Answer: C

Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 10

- (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 13

- (Exam Topic 1)

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated 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 15

- (Exam Topic 1)

The Firewall Administrator is required to create 100 new host objects with different IP addresses. What API command can he use in the script to achieve the requirement?

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

Answer:

A

NEW QUESTION 19

- (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 24

- (Exam Topic 1)

When requiring certificates for mobile devices, make sure the authentication method is set to one of the following, Username and Password, RADIUS or _____.

- A. SecureID
- B. SecurID
- C. Complexity
- D. TacAcs

Answer: B

NEW QUESTION 29

- (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 32

- (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 36

- (Exam Topic 1)

Which statement is correct about the Sticky Decision Function?

- A. It is not supported with either the Performance pack of a hardware based accelerator card
- B. Does not support SPI's when configured for Load Sharing
- C. It is automatically disabled if the Mobile Access Software Blade is enabled on the cluster
- D. It is not required L2TP traffic

Answer: A

NEW QUESTION 38

- (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 40

- (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 44

- (Exam Topic 1)

What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

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

Answer: C

Explanation:

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

NEW QUESTION 47

- (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 49

- (Exam Topic 1)

If you needed the Multicast MAC address of a cluster, what command would you run?

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

Answer: D

NEW QUESTION 53

- (Exam Topic 1)

What is not a component of Check Point SandBlast?

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

Answer: B

NEW QUESTION 55

- (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 57

- (Exam Topic 1)

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient
- D. Security Gateway
- E. SmartEvent

Answer: D

NEW QUESTION 61

- (Exam Topic 1)

Which of the following statements is TRUE about R81 management plug-ins?

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

Answer: C

NEW QUESTION 64

- (Exam Topic 1)

What is the correct command to observe the Sync traffic in a VRRP environment?

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

Answer: D

NEW QUESTION 65

- (Exam Topic 1)

Which of the following authentication methods ARE NOT used for Mobile Access?

- A. RADIUS server
- B. Username and password (internal, LDAP)
- C. SecurID
- D. TACACS+

Answer: D

NEW QUESTION 68

- (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 69

- (Exam Topic 1)

In R81 spoofing is defined as a method of:

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

Answer: D

Explanation:

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

NEW QUESTION 72

- (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 73

- (Exam Topic 1)

What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

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

Answer: A

NEW QUESTION 74

- (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 77

- (Exam Topic 2)

Which of these is an implicit MEP option?

- A. Primary-backup
- B. Source address based
- C. Round robin
- D. Load Sharing

Answer: A

NEW QUESTION 79

- (Exam Topic 2)

John is using Management HA. Which Smartcenter should be connected to for making changes?

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

Answer: B

NEW QUESTION 84

- (Exam Topic 2)

Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

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

Answer: C

NEW QUESTION 88

- (Exam Topic 2)

SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

- A. This statement is true because SecureXL does improve all traffic.
- B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
- C. This statement is true because SecureXL does improve this traffic.
- D. This statement is false because encrypted traffic cannot be inspected.

Answer: C

Explanation:

SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

NEW QUESTION 92

- (Exam Topic 2)

Which GUI client is supported in R81?

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

Answer: C

NEW QUESTION 95

- (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 100

- (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 104

- (Exam Topic 2)

You are investigating issues with to gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

- A. TCP port 443
- B. TCP port 257
- C. TCP port 256
- D. UDP port 8116

Answer: C

NEW QUESTION 109

- (Exam Topic 2)

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode.
- B. Install appliance TE250X in standalone mode and setup MTA.
- C. You can utilize only Check Point Cloud Services for this scenario.
- D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance.

Answer: C

NEW QUESTION 113

- (Exam Topic 2)

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
- D. Yes, but only one has the right to write.

Answer: C

NEW QUESTION 117

- (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 119

- (Exam Topic 2)

What is the command to see cluster status in cli expert mode?

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

Answer: D

NEW QUESTION 123

- (Exam Topic 2)

What is the purpose of extended master key extension/session hash?

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

Answer: B

NEW QUESTION 125

- (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 126

- (Exam Topic 2)

In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with _____ will not apply.

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

Answer: B

NEW QUESTION 127

- (Exam Topic 2)

Which encryption algorithm is the least secured?

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

Answer: C

NEW QUESTION 131

- (Exam Topic 2)

The Correlation Unit performs all but the following actions:

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

Answer: C

NEW QUESTION 136

- (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 139

- (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 140

- (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 145

- (Exam Topic 2)

With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

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

Answer: A

NEW QUESTION 147

- (Exam Topic 2)

Which directory below contains log files?

- A. /opt/CPSmartlog-R81/log
- B. /opt/CPshrd-R81/log
- C. /opt/CPsuite-R81/fw1/log
- D. /opt/CPsuite-R81/log

Answer: C

NEW QUESTION 149

- (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 153

- (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 158

- (Exam Topic 2)

Which statement is true about ClusterXL?

- A. Supports Dynamic Routing (Unicast and Multicast)
- B. Supports Dynamic Routing (Unicast Only)
- C. Supports Dynamic Routing (Multicast Only)
- D. Does not support Dynamic Routing

Answer: A

NEW QUESTION 161

- (Exam Topic 2)

Customer's R81 management server needs to be upgraded to R81.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R81 configuration, clean install R81.10 and import the configuration
- B. CPUSE offline upgrade
- C. CPUSE online upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 163

- (Exam Topic 2)

What are the steps to configure the HTTPS Inspection Policy?

- A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
- B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
- C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
- D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: A

NEW QUESTION 166

- (Exam Topic 2)

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

NEW QUESTION 168

- (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 172

- (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 176

- (Exam Topic 2)

Which one of the following is true about Threat Emulation?

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

Answer: D

NEW QUESTION 179

- (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 181

- (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 185

- (Exam Topic 2)

The following command is used to verify the CPUSE version:

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

Answer: A

NEW QUESTION 187

- (Exam Topic 3)

What cloud-based SandBlast Mobile application is used to register new devices and users?

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

Answer: D

NEW QUESTION 190

- (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 192

- (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 193

- (Exam Topic 3)

What will SmartEvent automatically define as events?

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

Answer:

C

NEW QUESTION 197

- (Exam Topic 3)

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

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

Answer: B

NEW QUESTION 198

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 202

- (Exam Topic 3)

Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.

What will happen to the changes already made?

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

Answer: A

NEW QUESTION 206

- (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 211

- (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 215

- (Exam Topic 3)

What key is used to save the current CPView page in a filename format cpview_ "cpview process ID".cap "number of captures"?

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

Answer: C

NEW QUESTION 219

- (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 220

- (Exam Topic 3)

Office mode means that:

- A. SecurID client assigns a routable MAC address
- B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
- C. Users authenticate with an Internet browser and use secure HTTPS connection.
- D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
- E. Allows a security gateway to assign a remote client an IP address
- F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

NEW QUESTION 223

- (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 225

- (Exam Topic 3)

What is not a purpose of the deployment of Check Point API?

- A. Execute an automated script to perform common tasks
- B. Create a customized GUI Client for manipulating the objects database
- C. Create products that use and enhance the Check Point solution
- D. Integrate Check Point products with 3rd party solution

Answer: B

NEW QUESTION 230

- (Exam Topic 3)

What kind of information would you expect to see using the sim affinity command?

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

Answer: D

NEW QUESTION 231

- (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 232

- (Exam Topic 3)

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine

- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

Answer: A

NEW QUESTION 235

- (Exam Topic 3)

What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

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

Answer: A

NEW QUESTION 237

- (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 242

- (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 247

- (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 249

- (Exam Topic 3)

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CApp

Answer: B

NEW QUESTION 254

- (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 258

- (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 260

- (Exam Topic 3)

What is the command to show SecureXL status?

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

Answer: D

Explanation:

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

NEW QUESTION 264

- (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 267

- (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 269

- (Exam Topic 3)

Which path below is available only when CoreXL is enabled?

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

Answer: C

NEW QUESTION 274

- (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 279

- (Exam Topic 3)

What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)

General					
Status	Name	IP	Version	Active Blade	
	A-GW	10.1.1.1	R80		
	SMS	10.1.1.101	R80		

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

Answer: B

NEW QUESTION 280

- (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 281

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 283

- (Exam Topic 4)

If SecureXL is disabled which path is used to process traffic?

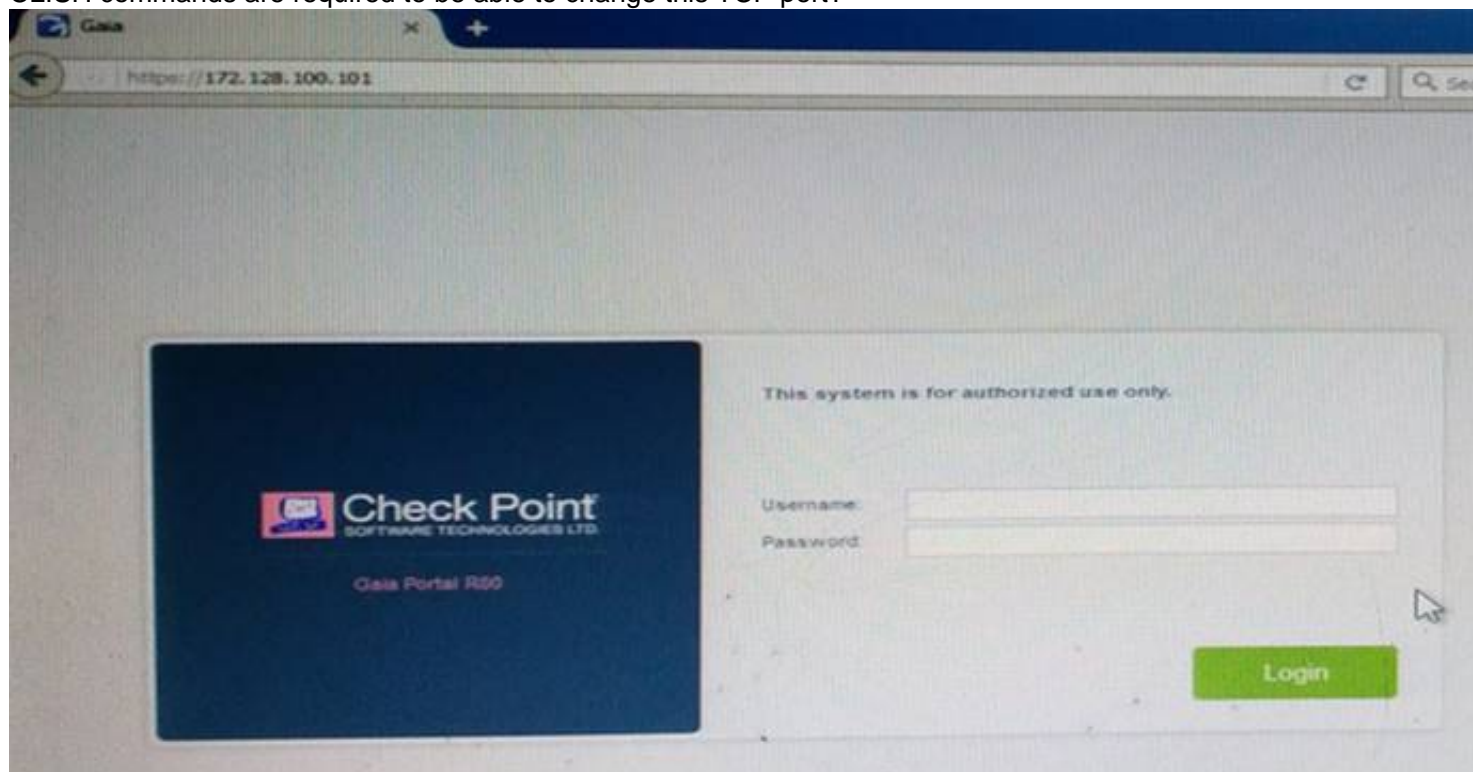
- A. Passive path
- B. Medium path
- C. Firewall path
- D. Accelerated path

Answer: C

NEW QUESTION 285

- (Exam Topic 4)

Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



- A. set web ssl-port <new port number>
- B. set Gaia-portal port <new port number>
- C. set Gaia-portal https-port <new port number>
- D. set web https-port <new port number>

Answer: A

NEW QUESTION 289

- (Exam Topic 4)

Installations and upgrades with CPUSE require that the CPUSE agent is up-to-date. Usually the latest build is downloaded automatically. How can you verify the CPUSE agent build?

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

Answer: A

NEW QUESTION 294

- (Exam Topic 4)

Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

- A. Formal; corporate
- B. Local; formal
- C. Local; central
- D. Central; local

Answer: D

NEW QUESTION 298

- (Exam Topic 4)

Which of the following Check Point commands is true to enable Multi-Version Cluster (MVC)?

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

Answer: D

NEW QUESTION 303

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 304

- (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 309

- (Exam Topic 4)

After having saved the Cllsh Configuration with the "save configuration config.txt*" command, where can you find the config.txt file?

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

Answer: B

NEW QUESTION 312

- (Exam Topic 4)

After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?

- A. You will find it in the home directory of your user account (e.
- B. /home/admin/)
- C. You can locate the file via SmartConsole > Command Line.
- D. You have to launch the WebUI and go to "Config" -> "Export Config File" and specify the destination directory of your local file system.
- E. You cannot locate the file in the file system since Clish does not have any access to the bash file system

Answer: A

NEW QUESTION 314

- (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 319

- (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 320

- (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 323

- (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 324

- (Exam Topic 4)

Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

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

Answer: D

NEW QUESTION 329

- (Exam Topic 4)

What is the purpose of the command "ps aux | grep twd"?

- A. You can check the Process ID and the processing time of the twd process.
- B. You can convert the log file into Post Script format.

- C. You can list all Process IDs for all running services.
- D. You can check whether the IPS default setting is set to Detect or Prevent mode

Answer: A

NEW QUESTION 332

- (Exam Topic 4)

GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

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

Answer: A

NEW QUESTION 337

- (Exam Topic 4)

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

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

Answer: B

Explanation:

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

NEW QUESTION 342

- (Exam Topic 4)

What are the correct steps upgrading a HA cluster (M1 is active. M2 is passive) using Multi-Version Cluster(MVC) Upgrade?

- A. 1) Enable the MVC mechanism on both cluster members «cphaprob mvc on2) Upgrade the passive node M2 to R81.103) In SmartConsol
- B. change the version of the cluster object4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism
- C. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on2) Upgrade the passive node M2 to R81.103) In SmartConsol
- D. change the version of the cluster object4) Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy
- E. 1) In SmartConsol
- F. change the version of the cluster object2) Upgrade the passive node M2 to R81.103) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 Wcphaconf mvc on4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsol
- G. change the version of the cluster object
- H. 1) Upgrade the passive node M2 to R81.102) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 ttcpchaconf mvc on3) In SmartConsole, change the version of the cluster object 4) Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.10

Answer: D

NEW QUESTION 347

- (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 350

- (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 351

- (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 354

- (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 357

- (Exam Topic 4)

Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

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

Answer: B

NEW QUESTION 361

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 366

- (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 369

- (Exam Topic 4)

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

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

Answer: B

NEW QUESTION 370

- (Exam Topic 4)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 371

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 372

- (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 377

- (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 380

- (Exam Topic 4)

SecureXL is able to accelerate the Connection Rate using templates. Which attrnbutes are used in the template to identify the connection?

- A. Source address . Destination address
- B. Source Port, Destination port
- C. Source address . Destination address
- D. Destination port
- E. Source address . Destination address
- F. Destination por
- G. Pro^col
- H. Source address . Destination address
- I. Source Port, Destination por
- J. Protocol

Answer: D

NEW QUESTION 384

- (Exam Topic 4)

What should the admin do in case the Primary Management Server is temporary down?

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

Answer: A

NEW QUESTION 389

- (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 390

- (Exam Topic 4)

Which of the following is NOT supported by CPUSE?

- A. Automatic download of full installation and upgrade packages
- B. Automatic download of hotfixes
- C. Installation of private hotfixes
- D. Offline installations

Answer: D

Explanation:

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

NEW QUESTION 392

- (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 396

- (Exam Topic 4)

When users connect to the Mobile Access portal they are unable to open File Shares. Which log file would you want to examine?

- A. cvpnd.elg
- B. httpd.elg
- C. vpnd.elg
- D. fw.elg

Answer: A

NEW QUESTION 401

- (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 404

- (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 406

- (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 411

- (Exam Topic 4)

What is the purpose of the CPCA process?





- A. Monitoring the status of processes.
- B. Sending and receiving logs.
- C. Communication between GUI clients and the SmartCenter server.
- D. Generating and modifying certificates.

Answer: D

NEW QUESTION 416

- (Exam Topic 4)

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

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

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

Answer: A

NEW QUESTION 417

- (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 418

- (Exam Topic 4)

Packet acceleration (SecureXL) identifies connections by several attributes- Which of the attributes is NOT used for identifying connection?

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

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 423

- (Exam Topic 4)

What is false regarding a Management HA environment?

- A. Only one Management Server should be active, while any others be in standby mode
- B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.
- C. SmartConsole can connect to any management server in Readonly mode.
- D. Synchronization will occur automatically with each Publish event if the Standby servers are available.

Answer: B

NEW QUESTION 428

- (Exam Topic 4)

What is the minimum number of CPU cores required to enable CoreXL?

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

Answer: C

Explanation:

Default number of CoreXL IPv4 FW instances:

Note: The real number of CoreXL FW instances depends on the current CoreXL license. Number of

CPU cores Default number of CoreXL IPv4

FW instances Default number of Secure Network Distributors (SNDs)

1 1

Note: CoreXL is disabled 0 Note: CoreXL is disabled

2 2 2

4 3 1

6 - 20 [Number of CPU cores] - 2 2

More than 20 (1) [Number of CPU cores] - 4 4

NEW QUESTION 429

- (Exam Topic 4)

Bob has finished to setup provisioning a secondary security management server. Now he wants to check if the provisioning has been correct. Which of the following Check Point command can be used to check if the security management server has been installed as a primary or a secondary security management server?

- A. cprod_util MgmtIsPrimary
- B. cprod_util FwIsSecondary
- C. cprod_util MgmtIsSecondary
- D. cprod_util FwIsPrimary

Answer: A

NEW QUESTION 431

- (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 436

- (Exam Topic 4)

Which command shows only the table names of all kernel tables?

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

Answer: A

NEW QUESTION 439

- (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 441

- (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 442

- (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 number
- 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 use
- 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 use
- 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 number
- H. In dish run `>show web daemon-enable` to see if the web daemon is enabled.

Answer: C

NEW QUESTION 443

- (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 444

- (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 448

- (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 451

- (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 453

- (Exam Topic 4)

Which software blade does NOT accompany the Threat Prevention policy?

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

Answer: D

NEW QUESTION 454

- (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 459

- (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 460

- (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 462

- (Exam Topic 4)

You want to allow your Mobile Access Users to connect to an internal file share. Adding the Mobile Application 'File Share' to your Access Control Policy in the SmartConsole didn't work. You will be only allowed to select Services for the 'Service & Application' column How to fix it?

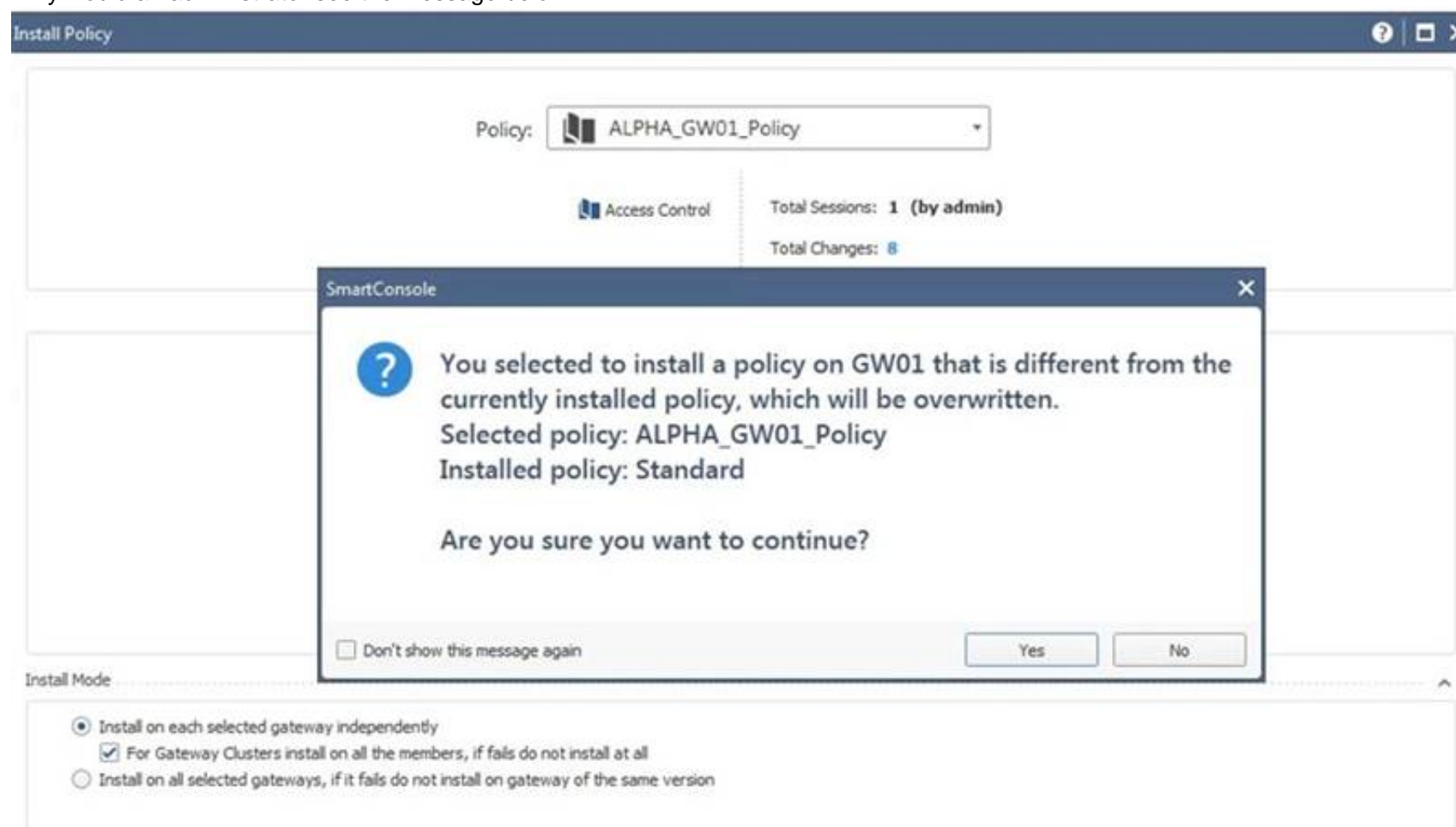
- A. A Quantum Spark Appliance is selected as Installation Target for the policy packet.
- B. The Mobile Access Blade is not enabled for the Access Control Layer of the policy.
- C. The Mobile Access Policy Source under Gateway properties Is set to Legacy Policy and not to Unified Access Policy.
- D. The Mobile Access Blade is not enabled under Gateway properties.

Answer: C

NEW QUESTION 467

- (Exam Topic 4)

Why would an administrator see the message below?



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

Answer: B

NEW QUESTION 469

- (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 473

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 477

- (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 479

- (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 482

- (Exam Topic 4)

What is the command to check the status of Check Point processes?

- A. top
- B. cptop
- C. cphaprob list
- D. cpwd_admin list

Answer: D

NEW QUESTION 484

- (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 487

- (Exam Topic 4)

What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

- A. CPUSE offline upgrade only

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

Answer: B

NEW QUESTION 490

- (Exam Topic 4)

In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?

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

Answer: C

Explanation:

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

NEW QUESTION 493

- (Exam Topic 4)

What destination versions are supported for a Multi-Version Cluster Upgrade?

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

Answer: D

NEW QUESTION 494

- (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 499

- (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 504

- (Exam Topic 4)

Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (EL-A) services.

- A. DASSERVICE
- B. FWD
- C. CPVIEWD
- D. CPD

Answer: A

NEW QUESTION 509

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 513

- (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 514

- (Exam Topic 4)

What is the amount of Priority Queues by default?

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

Answer: D

NEW QUESTION 519

- (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 522

- (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 526

- (Exam Topic 4)

Which one of the following is NOT a configurable Compliance Regulation?

- A. GLBA
- B. CJIS
- C. SOCI
- D. NCIPA

Answer: C

NEW QUESTION 527

- (Exam Topic 4)

What are the two types of tests when using the Compliance blade?

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

Answer: D

NEW QUESTION 532

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

156-315.81 Practice Exam Features:

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