

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

Which of the following is a new R81 Gateway feature that had not been available in R77.X and older?

- A. The rule base can be built of layers, each containing a set of the security rule
- B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- D. Time object to a rule to make the rule active only during specified times.
- E. Sub Policies are sets of rules that can be created and attached to specific rule
- F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

Which view is NOT a valid CPVIEW view?

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

Answer: C

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)

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 5

- (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 6

- (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 7

- (Exam Topic 1)

Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

- A. 15 sec
- B. 60 sec
- C. 5 sec

D. 30 sec

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

Which command collects diagnostic data for analyzing customer setup remotely?

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

Answer: A

Explanation:

CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

NEW QUESTION 9

- (Exam Topic 1)

Which features are only supported with R81.10 Gateways but not R77.x?

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 13

- (Exam Topic 1)

The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

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

Answer: D

NEW QUESTION 16

- (Exam Topic 1)

Which TCP-port does CPM process listen to?

- A. 18191
- B. 18190

C. 8983
D. 19009

Answer: D

NEW QUESTION 18

- (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 19

- (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 20

- (Exam Topic 1)

Which command will allow you to see the interface status?

- A. cphaprob interface
- B. cphaprob -l interface
- C. cphaprob -a if
- D. cphaprob stat

Answer: C

NEW QUESTION 24

- (Exam Topic 1)

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- B. Create a separate Security Policy package for each remote Security Gateway.
- C. Create network objects that restricts all applicable rules to only certain networks.
- D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Answer: B

NEW QUESTION 29

- (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 32

- (Exam Topic 1)

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

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

Answer: D

Explanation:

Synchronization works in two modes:

Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.

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

NEW QUESTION 33

- (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 34

- (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 38

- (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 42

- (Exam Topic 1)

Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?

- A. Severity
- B. Automatic reactions
- C. Policy
- D. Threshold

Answer: C

NEW QUESTION 47

- (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 50

- (Exam Topic 1)

Which statement is NOT TRUE about Delta synchronization?

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

Answer: A

NEW QUESTION 51

- (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 53

- (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 58

- (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 61

- (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 63

- (Exam Topic 1)

What is the limitation of employing Sticky Decision Function?

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

Answer: B

NEW QUESTION 68

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 73

- (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 77

- (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 82

- (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 85

- (Exam Topic 1)

Session unique identifiers are passed to the web api using which http header option?

- A. X-chkp-sid
- B. Accept-Charset
- C. Proxy-Authorization
- D. Application

Answer: C

NEW QUESTION 87

- (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 91

- (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 96

- (Exam Topic 1)

Which command lists all tables in Gaia?

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

Answer: C

NEW QUESTION 98

- (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 102

- (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 104

- (Exam Topic 1)

In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?

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

Answer: A

NEW QUESTION 106

- (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 111

- (Exam Topic 1)

Where you can see and search records of action done by R81 SmartConsole administrators?

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

Answer: B

NEW QUESTION 112

- (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 114

- (Exam Topic 1)

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 116

- (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 121

- (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 124

- (Exam Topic 1)

What is true about VRRP implementations?

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

Answer: C

NEW QUESTION 127

- (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 132

- (Exam Topic 2)

Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

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

Answer: D

NEW QUESTION 133

- (Exam Topic 2)

What are the blades of Threat Prevention?

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

Answer: D

NEW QUESTION 134

- (Exam Topic 2)

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

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

Answer: A

NEW QUESTION 135

- (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 139

- (Exam Topic 2)

An administrator would like to troubleshoot why templating is not working for some traffic. How can he determine at which rule templating is disabled?

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

Answer: D

NEW QUESTION 144

- (Exam Topic 2)

You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command. You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

- A. cphaprob -f register
- B. cphaprob -d -s report
- C. cpstat -f all
- D. cphaprob -a list

Answer: D

NEW QUESTION 147

- (Exam Topic 2)

Which of the following will NOT affect acceleration?

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

Answer: B

NEW QUESTION 150

- (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 is 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 153

- (Exam Topic 2)

Which of the following is NOT a type of Check Point API available in R81.x?

- A. Identity Awareness Web Services
- B. OPSEC SDK
- C. Mobile Access
- D. Management

Answer: C

NEW QUESTION 154

- (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 156

- (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 158

- (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 163

- (Exam Topic 2)

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

Answer: B

NEW QUESTION 168

- (Exam Topic 2)

Which command shows the current connections distributed by CoreXL FW instances?

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

Answer: A

NEW QUESTION 170

- (Exam Topic 2)

Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

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

Answer: A

NEW QUESTION 173

- (Exam Topic 2)

Which Check Point daemon monitors the other daemons?

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

Answer: C

NEW QUESTION 176

- (Exam Topic 2)

Which of the following is NOT a component of Check Point Capsule?

- A. Capsule Docs
- B. Capsule Cloud
- C. Capsule Enterprise
- D. Capsule Workspace

Answer: C

NEW QUESTION 181

- (Exam Topic 2)

When simulating a problem on ClusterXL cluster with cphaprob -d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

- A. cphaprob -d STOP unregister
- B. cphaprob STOP unregister
- C. cphaprob unregister STOP
- D. cphaprob -d unregister STOP

Answer: A

Explanation:

esting a failover in a controlled manner using following command;

cphaprob -d STOP -s problem -t 0 register

This will register a problem state on the cluster member this was entered on; If you then run;

cphaprob list

this will show an entry named STOP.

to remove this problematic register run following;

cphaprob -d STOP unregister References:

NEW QUESTION 183

- (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 187

- (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 190

- (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 193

- (Exam Topic 2)

What scenario indicates that SecureXL is enabled?

- A. Dynamic objects are available in the Object Explorer
- B. SecureXL can be disabled in cpconfig
- C. fwaccel commands can be used in clish
- D. Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 195

- (Exam Topic 2)

VPN Link Selection will perform the following when the primary VPN link goes down?

- A. The Firewall will drop the packets.
- B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
- C. The Firewall will send out the packet on all interfaces.
- D. The Firewall will inform the client that the tunnel is down.

Answer: B

NEW QUESTION 197

- (Exam Topic 2)

Which Remote Access Client does not provide an Office-Mode Address?

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

Answer: A

NEW QUESTION 199

- (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 201

- (Exam Topic 2)

What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?

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

Answer: D

NEW QUESTION 206

- (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 209

- (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 213

- (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 217

- (Exam Topic 2)

When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?

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

Answer: C

NEW QUESTION 222

- (Exam Topic 2)

Which command is used to display status information for various components?

- A. show all systems
- B. show system messages
- C. sysmess all
- D. show sysenv all

Answer: D

NEW QUESTION 225

- (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 227

- (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 229

- (Exam Topic 2)

John detected high load on sync interface. Which is most recommended solution?

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

D. For short connections like icmp service – delay sync for 2 seconds

Answer: A

NEW QUESTION 232

- (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 233

- (Exam Topic 2)

SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

- A. 19090,22
- B. 19190,22
- C. 18190,80
- D. 19009,443

Answer: D

NEW QUESTION 234

- (Exam Topic 2)

When installing a dedicated R81 SmartEvent server. What is the recommended size of the root partition?

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20GB
- D. At least 20GB

Answer: D

NEW QUESTION 235

- (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 238

- (Exam Topic 2)

What is the benefit of “fw monitor” over “tcpdump”?

- A. “fw monitor” reveals Layer 2 information, while “tcpdump” acts at Layer 3.
- B. “fw monitor” is also available for 64-Bit operating systems.
- C. With “fw monitor”, you can see the inspection points, which cannot be seen in “tcpdump”
- D. “fw monitor” can be used from the CLI of the Management Server to collect information from multiple gateways.

Answer: C

NEW QUESTION 239

- (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 243

- (Exam Topic 2)

SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

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

Answer: A

NEW QUESTION 245

- (Exam Topic 2)

What is the port used for SmartConsole to connect to the Security Management Server?

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

Answer: A

NEW QUESTION 247

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 251

- (Exam Topic 3)

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 255

- (Exam Topic 3)

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 258

- (Exam Topic 3)

You can access the ThreatCloud Repository from:

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

Answer: D

NEW QUESTION 259

- (Exam Topic 3)

What is true of the API server on R81.10?

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

Answer: D

NEW QUESTION 260

- (Exam Topic 3)

You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.

What must you do to get SIC to work?

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

Answer: C

NEW QUESTION 264

- (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 266

- (Exam Topic 3)

To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

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

Answer: D

NEW QUESTION 270

- (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 273

- (Exam Topic 3)

GAiA Software update packages can be imported and installed offline in situation where:

- A. Security Gateway with GAiA does NOT have SFTP access to Internet
- B. Security Gateway with GAiA does NOT have access to Internet.
- C. Security Gateway with GAiA does NOT have SSH access to Internet.
- D. The desired CPUSE package is ONLY available in the Check Point CLOUD.

Answer: B

NEW QUESTION 278

- (Exam Topic 3)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 282

- (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 286

- (Exam Topic 3)

What command would show the API server status?

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

Answer: C

NEW QUESTION 289

- (Exam Topic 3)

What is the minimum amount of RAM needed for a Threat Prevention Appliance?

- A. 6 GB
- B. 8GB with Gaia in 64-bit mode
- C. 4 GB
- D. It depends on the number of software blades enabled

Answer: C

NEW QUESTION 291

- (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 295

- (Exam Topic 3)

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.

What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

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

Answer: A

NEW QUESTION 298

- (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 303

- (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 306

- (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 307

- (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 312

- (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 317

- (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 319

- (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 321

- (Exam Topic 3)

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

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

Answer: B

NEW QUESTION 324

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

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

Answer: B

NEW QUESTION 329

- (Exam Topic 3)
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

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

Answer: B

NEW QUESTION 330

- (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 332

- (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 334

- (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 338

- (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 343

- (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 346

- (Exam Topic 3)

You want to verify if your management server is ready to upgrade to R81.10. What tool could you use in this process?

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

Answer: C

NEW QUESTION 350

- (Exam Topic 3)

Which is not a blade option when configuring SmartEvent?

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

Answer: B

Explanation:

On the Management tab, enable these Software Blades: References:

NEW QUESTION 352

- (Exam Topic 3)

With MTA (Mail Transfer Agent) enabled the gateways manages SMTP traffic and holds external email with potentially malicious attachments. What is required in order to enable MTA (Mail Transfer Agent) functionality in the Security Gateway?

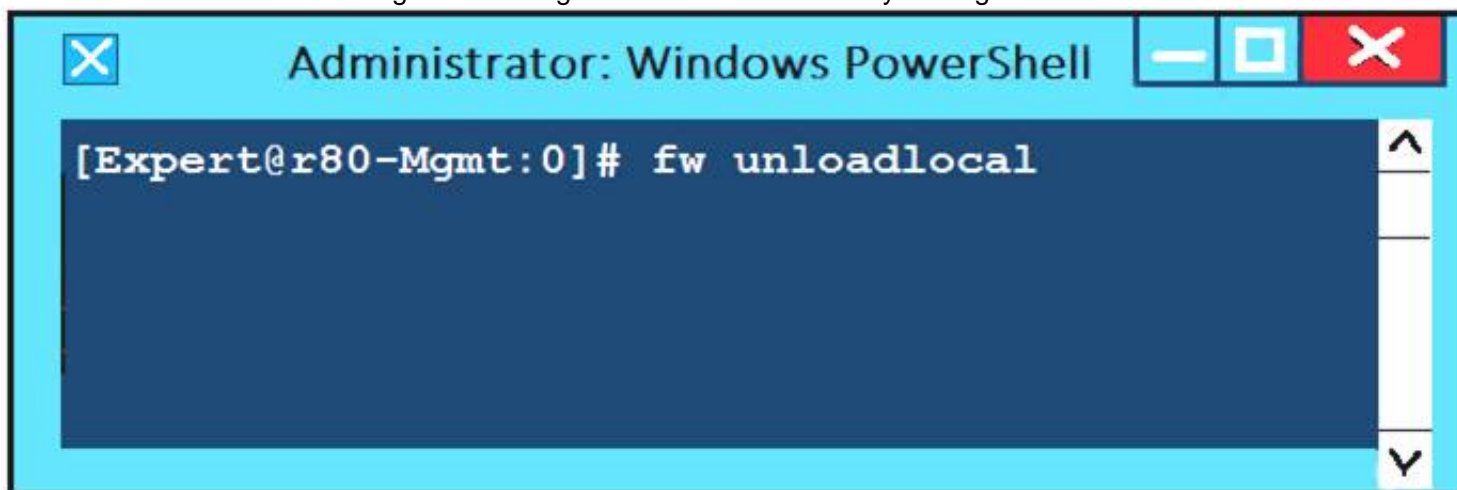
- A. Threat Cloud Intelligence
- B. Threat Prevention Software Blade Package
- C. Endpoint Total Protection
- D. Traffic on port 25

Answer: B

NEW QUESTION 356

- (Exam Topic 3)

What will be the effect of running the following command on the Security Management Server?



- A. Remove the installed Security Policy.
- B. Remove the local ACL lists.
- C. No effect.
- D. Reset SIC on all gateways.

Answer: A

NEW QUESTION 359

- (Exam Topic 3)

Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?

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

Answer: D

NEW QUESTION 362

- (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 364

- (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 367

- (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 372

- (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 374

- (Exam Topic 3)

For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

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

Answer: D

NEW QUESTION 376

- (Exam Topic 3)

What must you do first if "fwm sic_reset" could not be completed?

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

Answer: D

NEW QUESTION 377

- (Exam Topic 3)

Which is NOT an example of a Check Point API?

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

Answer: A

NEW QUESTION 378

- (Exam Topic 3)

You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

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

Answer: A

NEW QUESTION 380

- (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 383

- (Exam Topic 4)

Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command "cpconfig" to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances "Primary & Secondary" Which configuration option does she need to look for:

- A. Certificate's Fingerprint
- B. Random Pool
- C. CA Authority
- D. Certificate Authority

Answer: D

NEW QUESTION 386

- (Exam Topic 4)

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsive, which if these steps should NOT be performed:

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

Answer: A

NEW QUESTION 390

- (Exam Topic 4)

What is the default size of NAT table fw_x_alloc?

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

Answer: C

NEW QUESTION 395

- (Exam Topic 4)

Which command lists firewall chain?

- A. fwctl chain
- B. fw list chain
- C. fw chain module
- D. fw tab -t chainmod

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION 398

- (Exam Topic 4)

Which Check Point daemon invokes and monitors critical processes and attempts to restart them if they fail?

- A. fwm
- B. cpd

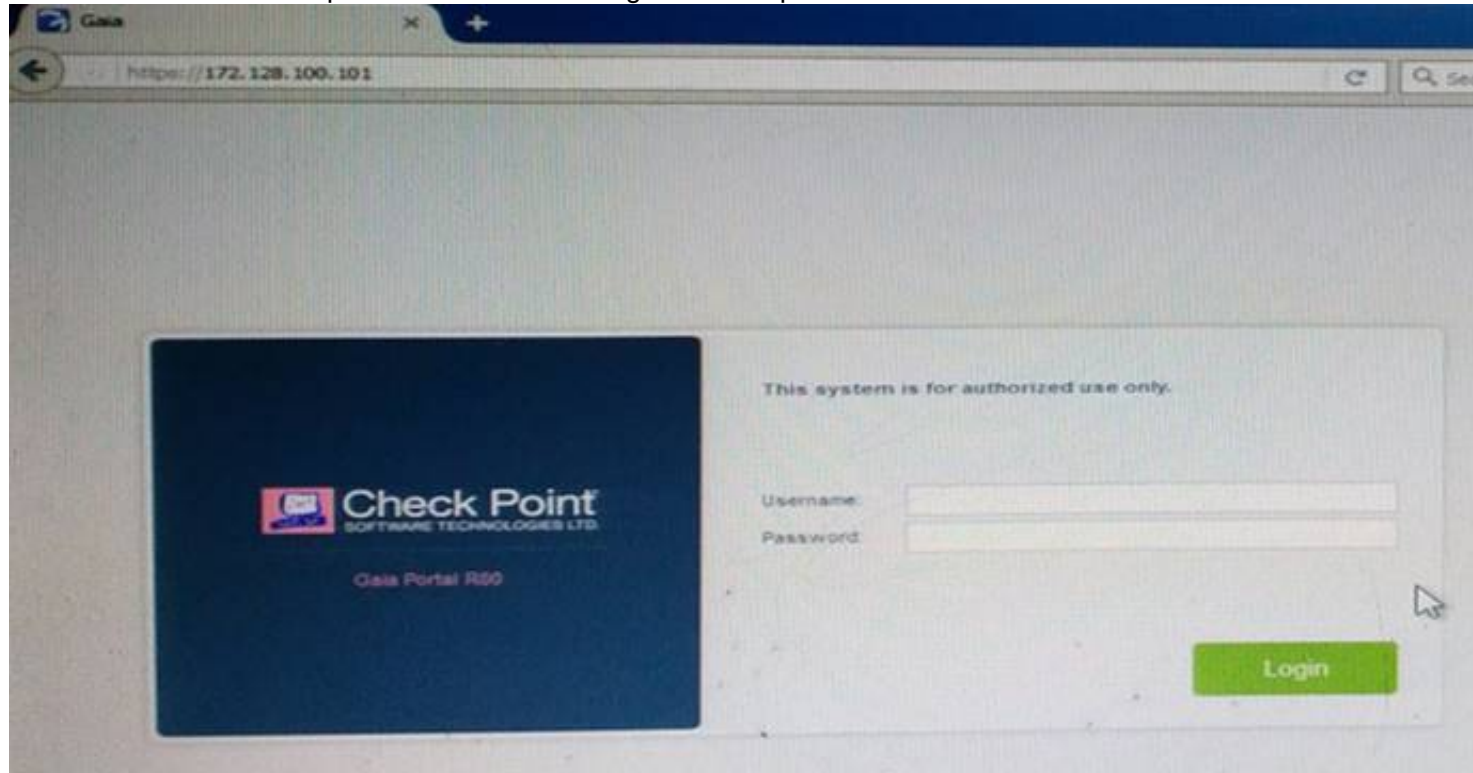
- C. cpwd
- D. cpm

Answer: C

NEW QUESTION 403

- (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 408

- (Exam Topic 4)

Which components allow you to reset a VPN tunnel?

- A. vpn tu command or SmartView monitor
- B. delete vpn ike sa or vpn she11 command
- C. vpn tunnelutil or delete vpn ike sa command
- D. SmartView monitor only

Answer: D

NEW QUESTION 412

- (Exam Topic 4)

The back end database for Check Point R81 Management uses:

- A. DBMS
- B. MongoDB
- C. PostgreSQL
- D. MySQL

Answer: C

NEW QUESTION 415

- (Exam Topic 4)

When using the Mail Transfer Agent, where are the debug logs stored?

- A. \$FWDIR/bin/emaild.mt
- B. elg
- C. \$FWDIR/log/mtad elg
- D. /var/log/mail.mta elg
- E. \$CPDIR/log/emaild elg

Answer: C

NEW QUESTION 418

- (Exam Topic 4)

How does the Anti-Virus feature of the Threat Prevention policy block traffic from infected websites?

- A. By dropping traffic from websites identified through ThreatCloud Verification and URL Caching
- B. By dropping traffic that is not proven to be from clean websites in the URL Filtering blade
- C. By allowing traffic from websites that are known to run Antivirus Software on servers regularly
- D. By matching logs against ThreatCloud information about the reputation of the website

Answer: D

NEW QUESTION 420

- (Exam Topic 4)

Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links.

Which component of SandBlast protection is her company using on a Gateway?

- A. SandBlast Threat Emulation
- B. SandBlast Agent
- C. Check Point Protect
- D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 423

- (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 428

- (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 431

- (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 433

- (Exam Topic 4)

You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.

What is the first step to run management API commands on GAIA's shell?

- A. mgmt_admin@teabag > id.txt
- B. mgmt_login
- C. login user admin password teabag
- D. mgmt_cli login user "admin" password "teabag" > id.txt

Answer: B

NEW QUESTION 438

- (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 440

- (Exam Topic 4)

When defining QoS global properties, which option below is not valid?

- A. Weight
- B. Authenticated timeout
- C. Schedule
- D. Rate

Answer: D

NEW QUESTION 445

- (Exam Topic 4)

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the tight protections in place. Check Point has been selected for the security vendor.

Which Check Point product protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS AND Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

Answer: D

NEW QUESTION 448

- (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 452

- (Exam Topic 4)

Matt wants to upgrade his old Security Management server to R81.x using the Advanced Upgrade with Database Migration. What is one of the requirements for a successful upgrade?

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

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/90083

NEW QUESTION 455

- (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 459

- (Exam Topic 4)

Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

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

Answer: A

NEW QUESTION 462

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 465

- (Exam Topic 4)

Which Queue in the Priority Queue has the maximum priority?

- A. High Priority
- B. Control
- C. Routing
- D. Heavy Data Queue

Answer: C

NEW QUESTION 466

- (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 470

- (Exam Topic 4)

The "Hit count" feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits if the Track option is set to "None"?

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

Answer: D

NEW QUESTION 474

- (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 478

- (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 481

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 482

- (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 485

- (Exam Topic 4)

What is a possible command to delete all of the SSH connections of a gateway?

- A. fw sam -l dport 22
- B. fw ctl conntab -x -dpott=22
- C. fw tab -t connections -x -e 00000016
- D. fwaccel dos config set dport ssh

Answer: A

NEW QUESTION 488

- (Exam Topic 4)

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

- A. ffffffff
- B. 00000001
- C. 00000002
- D. 00000003

Answer: B

NEW QUESTION 489

- (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 494

- (Exam Topic 4)

In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

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

Answer: D

NEW QUESTION 498

- (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 500

- (Exam Topic 4)

The admin is connected via ssh to 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 0.0.0.0:181        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 the 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 / 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 501

- (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 505

- (Exam Topic 4)

Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when _____.

- A. The license is attached to the wrong Security Gateway.
- B. The existing license expires.
- C. The license is upgraded.
- D. The IP address of the Security Management or Security Gateway has changed.

Answer: A

NEW QUESTION 507

- (Exam Topic 4)

Fill in the blank: An identity server uses a _____ for user authentication.

- A. Shared secret
- B. Certificate
- C. One-time password
- D. Token

Answer: A

NEW QUESTION 509

- (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 512

- (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 514

- (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 516

- (Exam Topic 4)

Which of the following is NOT an internal/native Check Point command?

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

Answer: C

NEW QUESTION 518

- (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 520

- (Exam Topic 4)

What feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?

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

Answer: B

NEW QUESTION 521

- (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 525

- (Exam Topic 4)

On R81.10 the IPS Blade is managed by:

- A. Threat Protection policy
- B. Anti-Bot Blade
- C. Threat Prevention policy
- D. Layers on Firewall policy

Answer: C

NEW QUESTION 526

- (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 527

- (Exam Topic 4)

The Compliance Blade allows you to search for text strings in many windows and panes, to search for a value in a field, what would your syntax be?

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

Answer: A

NEW QUESTION 530

- (Exam Topic 4)

What is the best sync method in the ClusterXL deployment?

- A. Use 1 cluster + 1st sync
- B. Use 1 dedicated sync interface
- C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
- D. Use 2 clusters +1st sync + 2nd sync

Answer: B

NEW QUESTION 534

- (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 536

- (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 537

- (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 540

- (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 544

- (Exam Topic 4)

In the R81 SmartConsole, on which tab are Permissions and Administrators defined?

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

Answer: C

NEW QUESTION 545

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

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG_R81
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/ cpconfig -> Enter the number of the Check Point

CoreXL option. (Enter 1 to select Change the number of firewall instances. OR Enter 2 for the option Change the number of IPv6 firewall instances.) -> Enter the total number of IPv4 (IPv6) CoreXL Firewall instances you wish the Security Gateway to run. Follow the instructions on the screen. -> Exit from the cpconfig menu.
- Reboot the Security Gateway.

NEW QUESTION 546

- (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 547

- (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 551

- (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 555

- (Exam Topic 4)

Which command is used to obtain the configuration lock in Gaia?

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

Answer: A

Explanation:

Obtaining a Configuration Lock

NEW QUESTION 558

- (Exam Topic 4)

When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

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

Answer: B

NEW QUESTION 561

- (Exam Topic 4)

Which component is NOT required to communicate with the Web Services API?

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

Answer: A

NEW QUESTION 563

- (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 568

- (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 571

- (Exam Topic 4)

What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

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

Answer: C

NEW QUESTION 575

- (Exam Topic 4)

Which 3 types of tracking are available for Threat Prevention Policy?

- A. SMS Alert, Log, SNMP alert
- B. Syslog, None, User-defined scripts
- C. None, Log, Syslog
- D. Alert, SNMP trap, Mail

Answer: B

NEW QUESTION 577

- (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 581

- (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 586

- (Exam Topic 4)

What needs to be configured if the NAT property 'Translate destination or client side' is not enabled in Global Properties?

- A. A host route to route to the destination IP.
- B. Use the file local.arp to add the ARP entries for NAT to work.
- C. Nothing, the Gateway takes care of all details necessary.
- D. Enabling 'Allow bi-directional NAT' for NAT to work correctly.

Answer: C

NEW QUESTION 591

- (Exam Topic 4)

What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

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

Answer: A

NEW QUESTION 595

- (Exam Topic 4)

When synchronizing clusters, which of the following statements is FALSE?

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

Answer: D

NEW QUESTION 599

- (Exam Topic 4)

When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

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

Answer: D

NEW QUESTION 600

- (Exam Topic 4)

By default, the R81 web API uses which content-type in its response?

- A. Java Script
- B. XML
- C. Text
- D. JSON

Answer: D

NEW QUESTION 603

- (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 606

- (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 610

- (Exam Topic 4)

When performing a minimal effort upgrade, what will happen to the network traffic?

- A. All connections that were initiated before the upgrade will be dropped, causing network downtime
- B. All connections that were initiated before the upgrade will be handled normally
- C. All connections that were initiated before the upgrade will be handled by the standby gateway
- D. All connections that were initiated before the upgrade will be handled by the active gateway

Answer: A

NEW QUESTION 615

- (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 619

- (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 624

- (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 628

- (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 629

- (Exam Topic 4)

Which is the correct order of a log flow processed by SmartEvent components?

- A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
- B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
- C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
- D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 633

- (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 634

- (Exam Topic 4)

SandBlast agent extends 0 day prevention to what part of the network?

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

Answer: A

NEW QUESTION 638

- (Exam Topic 4)

Main Mode in IKEv1 uses how many packages for negotiation?

- A. 4
- B. depends on the make of the peer gateway
- C. 3
- D. 6

Answer: C

NEW QUESTION 641

- (Exam Topic 4)

Is it possible to establish a VPN before the user login to the Endpoint Client?

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

Answer: D

NEW QUESTION 646

- (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

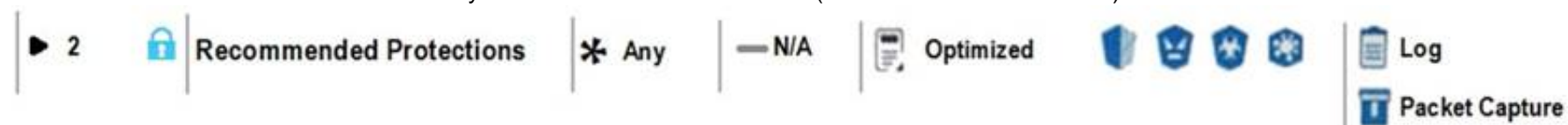
Explanation:

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

NEW QUESTION 651

- (Exam Topic 4)

View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



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

Answer: B

Explanation:

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

NEW QUESTION 653

- (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 656

- (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 660

- (Exam Topic 4)

What state is the Management HA in when both members have different policies/databases?

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

Answer: D

Explanation:

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

NEW QUESTION 663

- (Exam Topic 4)

Which of the following processes pulls the application monitoring status from gateways?

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

Answer: A

NEW QUESTION 664

- (Exam Topic 4)

If there are two administration logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available or other administrators? (Choose the BEST answer.)

- A. Publish or discard the session.
- B. Revert the session.
- C. Save and install the Policy.
- D. Delete older versions of database.

Answer: A

NEW QUESTION 666

- (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 667

- (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 672

- (Exam Topic 4)

When performing a minimal effort upgrade, what will happen to the network traffic?

- A. All connections that were Initiated before the upgrade will be dropped, causing network downtime.
- B. All connections that were initiated before the upgrade will be handled by the active gateway
- C. All connections that were initiated before the upgrade will be handled normally
- D. All connections that were initiated before the upgrade will be handled by the standby gateway

Answer: B

NEW QUESTION 675

- (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 680

- (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 681

- (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 683

- (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 687

- (Exam Topic 4)

After verifying that API Server is not running, how can you start the API Server?

- A. Run command "set api start" in CLISH mode
- B. Run command "mgmt cli set api start" in Expert mode
- C. Run command "mgmt api start" in CLISH mode
- D. Run command "api start" in Expert mode

Answer: B

NEW QUESTION 690

- (Exam Topic 4)

When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

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

Answer: C

NEW QUESTION 692

- (Exam Topic 4)

What are possible Automatic Reactions in SmartEvent?

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

Answer: A

NEW QUESTION 696

- (Exam Topic 4)

What is the correct description for the Dynamic Balancing / Split feature?

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

Answer: D

NEW QUESTION 701

- (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 706

- (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 711

- (Exam Topic 4)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

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

Answer: D

NEW QUESTION 716

- (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 718

- (Exam Topic 4)

In the Check Point Security Management Architecture, which component(s) can store logs?

- A. SmartConsole
- B. Security Management Server and Security Gateway
- C. Security Management Server
- D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 721

- (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 722

- (Exam Topic 4)

Fill in the blank: Authentication rules are defined for _____. .

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

Answer: A

NEW QUESTION 723

- (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 727

- (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 730

- (Exam Topic 4)

Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

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

Answer: A

NEW QUESTION 732

- (Exam Topic 4)

By default, which port does the WebUI listen on?

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

Answer: C

NEW QUESTION 734

- (Exam Topic 4)

What are the three SecureXL Templates available in R81.10?

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

Answer: B

NEW QUESTION 739

- (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 744

- (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 748

.....

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](#)