

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

Which is NOT an example of a Check Point API?

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

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

Which view is NOT a valid CPVIEW view?

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

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

Which of these statements describes the Check Point ThreatCloud?

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

Answer: D

NEW QUESTION 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)

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

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

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

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 7

- (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 8

- (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 9

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Which command can you use to verify the number of active concurrent connections?

- A. fw conn all
- B. fw ctl pstat
- C. show all connections
- D. show connections

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

The Security Gateway is installed on GAIA R81. The default port for the Web User Interface is _____.

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

Answer: D

NEW QUESTION 12

- (Exam Topic 1)

What is the mechanism behind Threat Extraction?

- A. This a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender.
- B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient.
- C. This is a new mechanism to identify the IP address of the sender of malicious codes and put it into the SAM database (Suspicious Activity Monitoring).
- D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast.

Answer: D

NEW QUESTION 15

- (Exam Topic 1)

On R81.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

- A. 18210
- B. 18184
- C. 257
- D. 18191

Answer: B

NEW QUESTION 20

- (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 21

- (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 22

- (Exam Topic 1)

During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

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

Answer: D

NEW QUESTION 24

- (Exam Topic 1)

There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?

- A. Using Web Services
- B. Using Mgmt_cli tool
- C. Using CLISH
- D. Using SmartConsole GUI console
- E. Events are collected with SmartWorkflow from Trouble Ticket systems

Answer: E

NEW QUESTION 28

- (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 31

- (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 34

- (Exam Topic 1)

SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data. Which component is NOT part of the SandBlast Mobile solution?

- A. Management Dashboard
- B. Gateway
- C. Personal User Storage
- D. Behavior Risk Engine

Answer: C

NEW QUESTION 38

- (Exam Topic 1)

The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

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

Answer: A

NEW QUESTION 39

- (Exam Topic 1)

Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 44

- (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 46

- (Exam Topic 1)

Which command shows actual allowed connections in state table?

- A. fw tab -t StateTable
- B. fw tab -t connections
- C. fw tab -t connection
- D. fw tab connections

Answer: B

NEW QUESTION 47

- (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 52

- (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 54

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 59

- (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 64

- (Exam Topic 1)

What are the three components for Check Point Capsule?

- A. Capsule Docs, Capsule Cloud, Capsule Connect
- B. Capsule Workspace, Capsule Cloud, Capsule Connect
- C. Capsule Workspace, Capsule Docs, Capsule Connect
- D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 66

- (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 69

- (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 74

- (Exam Topic 1)

What is the difference between an event and a log?

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow form Trouble Ticket systems
- D. Log and Events are synonyms

Answer: B

NEW QUESTION 76

- (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 77

- (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 81

- (Exam Topic 1)

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the “mgmt_cli” command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia’s secure shell(clish)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 84

- (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 89

- (Exam Topic 1)

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 94

- (Exam Topic 1)

To fully enable Dynamic Dispatcher on a Security Gateway:

- A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
- B. Using cpconfig, update the Dynamic Dispatcher value to “full” under the CoreXL menu.
- C. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
- D. run fw multik set_mode 1 in Expert mode and then reboot.

Answer: A

NEW QUESTION 95

- (Exam Topic 1)

Which packet info is ignored with Session Rate Acceleration?

- A. source port ranges
- B. source ip
- C. source port

D. same info from Packet Acceleration is used

Answer: B

NEW QUESTION 98

- (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 101

- (Exam Topic 1)

CPM process stores objects, policies, users, administrators, licenses and management data in a database. The database is:

- A. MySQL
- B. Postgres SQL
- C. MarisDB
- D. SOLR

Answer: B

NEW QUESTION 103

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 104

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 105

- (Exam Topic 2)

As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?

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

Answer: C

NEW QUESTION 106

- (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 107

- (Exam Topic 2)

Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

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

Answer: D

Explanation:

Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that require direct GUI access, such as SmartEvent, It provides the following:

- GUI Client communication
- Database manipulation
- Policy Compilation
- Management HA sync

NEW QUESTION 110

- (Exam Topic 2)

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats.
- B. Proactively detects threats.
- C. Delivers file with original content.
- D. Delivers PDF versions of original files with active content removed.

Answer: B

NEW QUESTION 114

- (Exam Topic 2)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

Answer: D

NEW QUESTION 115

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 118

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 123

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 124

- (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 128

- (Exam Topic 2)

How do Capsule Connect and Capsule Workspace differ?

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

Answer: A

NEW QUESTION 131

- (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 136

- (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 138

- (Exam Topic 2)

SmartEvent does NOT use which of the following procedures to identify events:

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

Answer: C

Explanation:

Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:

- Matching a Log Against Global Exclusions
- Matching a Log Against Each Event Definition
- Creating an Event Candidate
- When a Candidate Becomes an Event References:

NEW QUESTION 143

- (Exam Topic 2)

What is mandatory for ClusterXL to work properly?

- A. The number of cores must be the same on every participating cluster node
- B. The Magic MAC number must be unique per cluster node
- C. The Sync interface must not have an IP address configured
- D. If you have “Non-monitored Private” interfaces, the number of those interfaces must be the same on all cluster members

Answer: B

NEW QUESTION 145

- (Exam Topic 2)

From SecureXL perspective, what are the tree paths of traffic flow:

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

Answer: D

NEW QUESTION 149

- (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 151

- (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 155

- (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 158

- (Exam Topic 2)

Which one of the following is true about Capsule Connect?

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

Answer: A

NEW QUESTION 160

- (Exam Topic 2)

Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

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

Answer: B

Explanation:

Example:

mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json

- "--format json" is optional. By default the output is presented in plain text.

NEW QUESTION 165

- (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 169

- (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 172

- (Exam Topic 2)

What is the difference between SSL VPN and IPSec VPN?

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

Answer: D

NEW QUESTION 177

- (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 179

- (Exam Topic 2)

Which of the following links will take you to the SmartView web application?

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

Answer: B

NEW QUESTION 182

- (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 185

- (Exam Topic 2)

What is the benefit of “tw 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 186

- (Exam Topic 2)

The following command is used to verify the CPUSE version:

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

Answer: A

NEW QUESTION 189

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 194

- (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 197

- (Exam Topic 3)

On what port does the CPM process run?

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

Answer: D

NEW QUESTION 201

- (Exam Topic 3)

Joey wants to upgrade from R75.40 to R81 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this.

What is one of the requirements for his success?

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

Answer: B

NEW QUESTION 204

- (Exam Topic 3)

Which Check Point software blade provides Application Security and identity control?

- A. Identity Awareness
- B. Data Loss Prevention
- C. URL Filtering
- D. Application Control

Answer: D

NEW QUESTION 207

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 209

- (Exam Topic 3)

What is the Implicit Clean-up Rule?

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

Answer: C

NEW QUESTION 212

- (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 215

- (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 219

- (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 221

- (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 224

- (Exam Topic 3)

Fill in the blank: The “fw monitor” tool can be best used to troubleshoot _____.

- A. AV issues
- B. VPN errors
- C. Network traffic issues
- D. Authentication issues

Answer: C

Explanation:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

NEW QUESTION 225

- (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 229

- (Exam Topic 3)

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAI/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 233

- (Exam Topic 3)

One of major features in R81 SmartConsole is concurrent administration.

Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

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

Answer: C

NEW QUESTION 234

- (Exam Topic 3)

Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is _____ .

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

Answer: D

NEW QUESTION 235

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 236

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 240

- (Exam Topic 3)

Office mode means that:

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

Answer: D

NEW QUESTION 241

- (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 243

- (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 244

- (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 248

- (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 251

- (Exam Topic 3)

Which of the following commands shows the status of processes?

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

Answer: D

NEW QUESTION 254

- (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 259

- (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 260

- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

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

Answer: D

NEW QUESTION 261

- (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 264

- (Exam Topic 3)

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment.

Which details she need to fill in System Restore window before she can click OK button and test the backup?

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

Answer: C

NEW QUESTION 267

- (Exam Topic 3)

Ken wants to obtain a configuration lock from other administrator on R81 Security Management Server. He can do this via WebUI or via CLI.

Which command should he use in CLI? (Choose the correct answer.)

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

Answer: D

NEW QUESTION 268

- (Exam Topic 3)

What are the methods of SandBlast Threat Emulation deployment?

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

Answer: A

NEW QUESTION 271

- (Exam Topic 4)

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

- A. 224.0.0.18
- B. 224 00 5

- C. 224.0.0.102
- D. 224.0.0.22

Answer: A

NEW QUESTION 274

- (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 277

- (Exam Topic 4)

When Configuring Endpoint Compliance Settings for Applications and Gateways within Mobile Access, which of the three approaches will allow you to configure individual policies for each application?

- A. Basic Approach
- B. Strong Approach
- C. Very Advanced Approach
- D. Medium Approach

Answer: C

NEW QUESTION 278

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 280

- (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 283

- (Exam Topic 4)

Which of the following is NOT a type of Endpoint Identity Agent?

- A. Terminal
- B. Light
- C. Full
- D. Custom

Answer: A

NEW QUESTION 286

- (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 291

- (Exam Topic 4)

Bob works for a big security outsourcing provider company and as he receives a lot of change requests per day he wants to use for scripting daily tasks the API services (torn Check Point for the GAIA API. Firstly he needs to be aware if the API services are running for the GAIA operating system. Which of the following Check Point Command is true:

- A. gala_dlish status
- B. status gaiaapi
- C. api_gala status
- D. gala_api status

Answer: A

NEW QUESTION 292

- (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 295

- (Exam Topic 4)

Which feature is NOT provided by all Check Point Mobile Access solutions?

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

Answer: A

Explanation:

Types of Solutions

All of Check Point's Remote Access solutions provide:

NEW QUESTION 299

- (Exam Topic 4)

What are the services used for Cluster Synchronization?

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

Answer: C

NEW QUESTION 300

- (Exam Topic 4)

Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances Steve's manager. Diana asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?

- A. fw tab -t connections -s
- B. fw tab -t connections
- C. fw tab -t connections -c
- D. fw tab -t connections -f

Answer: B

NEW QUESTION 301

- (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 304

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 307

- (Exam Topic 4)

How long may verification of one file take for Sandblast Threat Emulation?

- A. up to 1 minutes
- B. within seconds cleaned file will be provided
- C. up to 5 minutes
- D. up to 3 minutes

Answer: B

NEW QUESTION 308

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 312

- (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 313

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 317

- (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 322

- (Exam Topic 4)

Packet acceleration (SecureXL) identifies 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 325

- (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 327

- (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 329

- (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 331

- (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 336

- (Exam Topic 4)

You need to change the MAC-address on eth2 interface of the gateway. What is the correct way to change MAC-address in Check Point Gaia?

- A. In CLISH run: set interface eth2 mac-addr 11:11:11:11:11:11
- B. In expert-mode run ifconfig eth1 hw 11:11:11:11 11 11
- C. In CLISH run set interface eth2 hw-addr 11 11 11:11:11 11
- D. In expert-mode run: ethtool -4 eth2 mac 11 11:11:11:11:11

Answer: A

NEW QUESTION 341

- (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 345

- (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 346

- (Exam Topic 4)

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

What can we infer about the recent changes made to the Rule Base?

- A. Rule 7 was created by the 'admin' administrator in the current session
- B. 8 changes have been made by administrators since the last policy installation
- C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
- D. Rule 1 and object webserver are locked by another administrator

Answer: D

NEW QUESTION 347

- (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 348

- (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 349

- (Exam Topic 4)

According to out of the box SmartEvent policy, which blade will automatically be correlated into events?

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

Answer: C

NEW QUESTION 350

- (Exam Topic 4)

Which Correction mechanisms are available with ClusterXL under R81.10?

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

Answer: C

NEW QUESTION 354

- (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 357

- (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 359

- (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 363

- (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 365

- (Exam Topic 4)

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.

- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server.

Answer: D

NEW QUESTION 367

- (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 368

- (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 373

- (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 375

- (Exam Topic 4)

John is using Management HA. Which Security Management Server should he use for making changes?

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

Answer: B

NEW QUESTION 378

- (Exam Topic 4)

What is false regarding a Management HA environment?

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

Answer: B

NEW QUESTION 380

- (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 382

- (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 383

- (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 388

- (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 390

- (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 394

- (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 399

- (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 401

- (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 404

- (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 405

- (Exam Topic 4)

You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R81 gateways.

Answer: A

NEW QUESTION 410

- (Exam Topic 4)

How can you switch the active log file?

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

Answer: D

NEW QUESTION 412

- (Exam Topic 4)

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

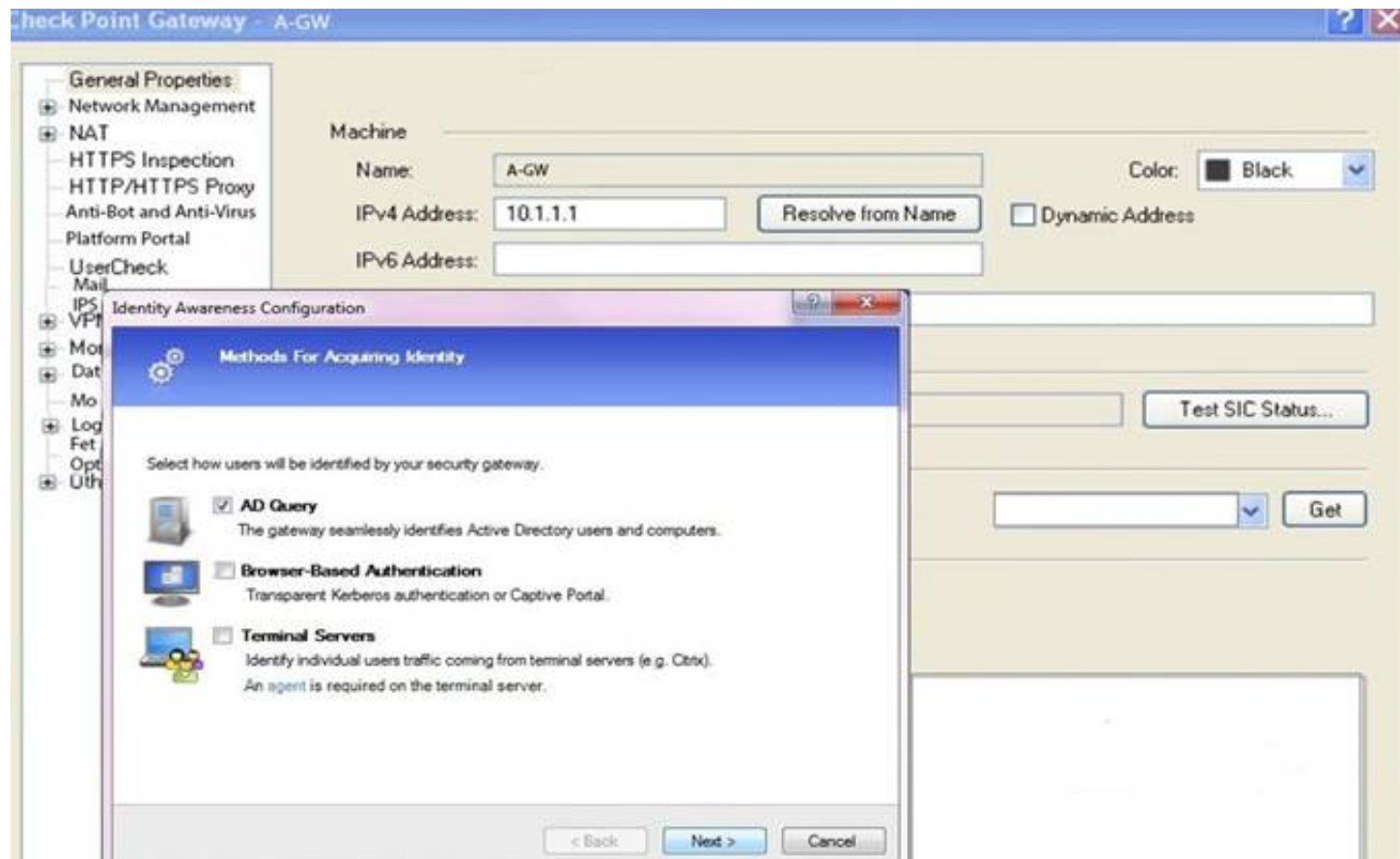
- A. ReverseCLIProxy
- B. ReverseProxyCLI
- C. ReverseProxy
- D. ProxyReverseCLI

Answer: C

NEW QUESTION 415

- (Exam Topic 4)

On the following picture an administrator configures Identity Awareness:



After clicking “Next” the above configuration is supported by:

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.
- C. Obligatory usage of Captive Portal.
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Answer: B

NEW QUESTION 418

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 421

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 424

- (Exam Topic 4)

At what point is the Internal Certificate Authority (ICA) created?

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

Answer: B

NEW QUESTION 426

- (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 430

- (Exam Topic 4)

What are possible Automatic Reactions in SmartEvent?

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

Answer: A

NEW QUESTION 434

- (Exam Topic 4)

To optimize Rule Base efficiency, the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

Answer: C

NEW QUESTION 438

- (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 443

- (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 448

- (Exam Topic 4)

The "MAC magic" value must be modified under the following condition:

- A. There is more than one cluster connected to the same VLAN
- B. A firewall cluster is configured to use Multicast for CCP traffic
- C. There are more than two members in a firewall cluster
- D. A firewall cluster is configured to use Broadcast for CCP traffic

Answer: D

NEW QUESTION 450

- (Exam Topic 4)

Fill in the blank: _____ information is included in "Full Log" tracking option, but is not included in "Log" tracking option?

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

Answer: B

NEW QUESTION 452

- (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 456

- (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 457

- (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 459

- (Exam Topic 4)

Which command shows the current Security Gateway Firewall chain?

- A. show current chain
- B. show firewall chain
- C. fw ctl chain
- D. fw ctl firewall-chain

Answer: C

NEW QUESTION 464

- (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 465

.....

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](#)