



# CheckPoint

## Exam Questions 156-315.81

Check Point Certified Security Expert R81

#### NEW QUESTION 1

- (Exam Topic 1)

Which is NOT an example of a Check Point API?

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

**Answer: A**

#### NEW QUESTION 2

- (Exam Topic 1)

Which of 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 3

- (Exam Topic 1)

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

- A. cphaprob set\_ccp multicast
- B. cphaconf set\_ccp multicast
- C. cphaconf set\_ccp no\_broadcast
- D. cphaprob set\_ccp no\_broadcast

**Answer: B**

#### NEW QUESTION 4

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 5

- (Exam Topic 1)

Which CLI command will reset the IPS pattern matcher statistics?

- A. ips reset pmstat
- B. ips pstats reset
- C. ips pmstats refresh
- D. ips pmstats reset

**Answer: D**

#### NEW QUESTION 6

- (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 7

- (Exam Topic 1)

Fill in the blank: The command \_\_\_\_\_ provides the most complete restoration of a R81 configuration.

- A. upgrade\_import
- B. cpconfig
- C. fwm dbimport -p <export file>

D. cpinfo –recover

**Answer:** A

#### NEW QUESTION 8

- (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 9

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 10

- (Exam Topic 1)

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 10

- (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 11

- (Exam Topic 1)

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

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

**Answer:** B

#### NEW QUESTION 12

- (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 14

- (Exam Topic 1)

Which of the following process pulls application monitoring status?

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

**Answer:** D

#### NEW QUESTION 15

- (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 19

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 22

- (Exam Topic 1)

Which command would disable a Cluster Member permanently?

- A. clusterXL\_admin down
- B. cphaprob\_admin down
- C. clusterXL\_admin down-p
- D. set clusterXL down-p

**Answer:** C

#### NEW QUESTION 25

- (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 27

- (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 32

- (Exam Topic 1)

The Event List within the Event tab contains:

- A. a list of options available for running a query.
- B. the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
- C. events generated by a query.
- D. the details of a selected event.

**Answer:** C

#### NEW QUESTION 33

- (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 35

- (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 37

- (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 39

- (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 44

- (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 49

- (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 51

- (Exam Topic 2)

Which GUI client is supported in R81?

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

**Answer:** C

**NEW QUESTION 53**

- (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 57**

- (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 61**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 66**

- (Exam Topic 2)

How often does Threat Emulation download packages by default?

- A. Once a week
- B. Once an hour
- C. Twice per day
- D. Once per day

**Answer:** D

**NEW QUESTION 67**

- (Exam Topic 2)

What is the name of the secure application for Mail/Calendar for mobile devices?

- A. Capsule Workspace
- B. Capsule Mail
- C. Capsule VPN
- D. Secure Workspace

**Answer:** A

**NEW QUESTION 68**

- (Exam Topic 2)

You have existing dbedit scripts from R77. Can you use them with R81.10?

- A. dbedit is not supported in R81.10
- B. dbedit is fully supported in R81.10
- C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
- D. dbedit scripts are being replaced by mgmt\_cli in R81.10

**Answer:** D

**NEW QUESTION 69**

- (Exam Topic 2)

Which encryption algorithm is the least secured?

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

**Answer: C**

#### NEW QUESTION 71

- (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 72

- (Exam Topic 2)

What is a best practice before starting to troubleshoot using the "fw monitor" tool?

- A. Run the command: fw monitor debug on
- B. Clear the connections table
- C. Disable CoreXL
- D. Disable SecureXL

**Answer: D**

#### NEW QUESTION 76

- (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 77

- (Exam Topic 2)

Which Check Point daemon monitors the other daemons?

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

**Answer: C**

#### NEW QUESTION 81

- (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 82

- (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 87

- (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 91**

- (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 95**

- (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 100**

- (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 101**

- (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 104**

- (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 109**

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 110

- (Exam Topic 2)

What are the steps to configure the HTTPS Inspection Policy?

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

**Answer: A**

#### NEW QUESTION 112

- (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 114

- (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 116

- (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 119

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 123

- (Exam Topic 2)

How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

- A. cphaprob set int fwaha\_vmac\_global\_param\_enabled 1
- B. clusterXL set int fwaha\_vmac\_global\_param\_enabled 1
- C. fw ctl set int fwaha\_vmac\_global\_param\_enabled 1
- D. cphaconf set int fwaha\_vmac\_global\_param\_enabled 1

**Answer: C**

#### NEW QUESTION 126

- (Exam Topic 2)

After making modifications to the \$CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

- A. cvpnd\_restart
- B. cvpnd\_restart
- C. cvpnd restart
- D. cvpnrestart

**Answer: B**

#### NEW QUESTION 131

- (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 134

- (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 137

- (Exam Topic 3)

Which is NOT a SmartEvent component?

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

**Answer: C**

#### NEW QUESTION 141

- (Exam Topic 3)

Please choose the path to monitor the compliance status of the Check Point R81.10 based management.

- A. Gateways & Servers --> Compliance View
- B. Compliance blade not available under R81.10
- C. Logs & Monitor --> New Tab --> Open compliance View
- D. Security & Policies --> New Tab --> Compliance View

**Answer: C**

#### NEW QUESTION 143

- (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 146

- (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 149

- (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 151

- (Exam Topic 3)

You have a Gateway is running with 2 cores. You plan to add a second gateway to build a cluster and used a device with 4 cores. How many cores can be used in a Cluster for Firewall-kernel on the new device?

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

**Answer:** D

#### NEW QUESTION 154

- (Exam Topic 3)

Which process handles connection from SmartConsole R81?

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

**Answer:** C

#### NEW QUESTION 155

- (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 157

- (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](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583)

#### NEW QUESTION 161

- (Exam Topic 3)

Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R81.

What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81?

- A. Missing an installed R77.20 Add-on on Security Management Server
- B. Unsupported firmware on UTM-1 Edge-W appliance
- C. Unsupported version on UTM-1 570 series appliance
- D. Unsupported appliances on remote locations

**Answer:** A

#### NEW QUESTION 166

- (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 169**

- (Exam Topic 3)

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

**Answer:** D

**NEW QUESTION 173**

- (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 174**

- (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 179**

- (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 182**

- (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 187**

- (Exam Topic 3)

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki

- C. Application Library
- D. CPApp

**Answer: B**

#### NEW QUESTION 192

- (Exam Topic 3)

What is the SandBlast Agent designed to do?

- A. Performs OS-level sandboxing for SandBlast Cloud architecture
- B. Ensure the Check Point SandBlast services is running on the end user's system
- C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network
- D. Clean up email sent with malicious attachments

**Answer: C**

#### NEW QUESTION 194

- (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 195

- (Exam Topic 3)

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

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

- A. There is a virus found
- B. Traffic is still allowed but not accelerated.
- C. The connection required a Security server.
- D. Acceleration is not enabled.
- E. The traffic is originating from the gateway itself.

**Answer: B**

#### NEW QUESTION 197

- (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 198

- (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 202

- (Exam Topic 3)

In ClusterXL Load Sharing Multicast Mode:

- A. only the primary member received packets sent to the cluster IP address
- B. only the secondary member receives packets sent to the cluster IP address
- C. packets sent to the cluster IP address are distributed equally between all members of the cluster
- D. every member of the cluster received all of the packets sent to the cluster IP address

**Answer: D**

#### NEW QUESTION 204

- (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 205

- (Exam Topic 3)

When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

- A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
- B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
- C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
- D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

**Answer: D**

#### NEW QUESTION 208

- (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 209

- (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 214

- (Exam Topic 3)

Which of the following is NOT an alert option?

- A. SNMP
- B. High alert
- C. Mail
- D. User defined alert

**Answer: B**

#### NEW QUESTION 219

- (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 220

- (Exam Topic 3)

With SecureXL enabled, accelerated packets will pass through the following:

- A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
- B. Network Interface Card, Check Point Firewall Kernel, and the Acceleration Device
- C. Network Interface Card and the Acceleration Device

D. Network Interface Card, OSI Network Layer, and the Acceleration Device

**Answer:** C

**NEW QUESTION 222**

- (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 227**

- (Exam Topic 3)

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



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

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

**Answer:** B

**NEW QUESTION 230**

- (Exam Topic 4)

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

**Answer:** B

**NEW QUESTION 233**

- (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 234**

- (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 237**

- (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 242

- (Exam Topic 4)

A user complains that some Internet resources are not available. The Administrator is having issues seeing it packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?

- A. run "fw unloadlocal" on the relevant gateway and check the ping again
- B. run "cpstop" on the relevant gateway and check the ping again
- C. run "fw log" on the relevant gateway
- D. run "fw ctl zdebug drop" on the relevant gateway

**Answer: D**

#### NEW QUESTION 247

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 250

- (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 252

- (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 254

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 255

- (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 256**

- (Exam Topic 4)

What are the modes of SandBlast Threat Emulation deployment?

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

**Answer: D**

**NEW QUESTION 260**

- (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 265**

- (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 266**

- (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 267**

- (Exam Topic 4)

What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

- A. Mutually Trusted Certificate Authorities
- B. Shared User Certificates
- C. Shared Secret Passwords
- D. Unique Passwords

**Answer: A**

**NEW QUESTION 272**

- (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 276**

- (Exam Topic 4)

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

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

**Answer:** B

**Explanation:**

Reference : [https://sc1.checkpoint.com/documents/R76/CP\\_R76\\_IdentityAwareness\\_AdminGuide/62402.htm](https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm)

**NEW QUESTION 280**

- (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 281**

- (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 282**

- (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 285**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 289**

- (Exam Topic 4)

Alice works for a big security outsourcing provider company and as she receives a lot of change requests per day she wants to use for scripting daily (asks the API services from Check Point for the Management API. Firstly she needs to be aware if the API services are running for the management. Which of the following Check Point Command is true:

- A. api mgmt status
- B. api status
- C. status api
- D. status mgmt apt

**Answer:** B

**NEW QUESTION 290**

- (Exam Topic 4)

Which process handles connection from SmartConsole R81?

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

**Answer:** C

#### NEW QUESTION 293

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

**Answer: D**

#### NEW QUESTION 298

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 301

- (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 304

- (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 309

- (Exam Topic 4)

If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

- A. Nothing - the proxy ARP is automatically handled in the R81 version
- B. Add the proxy ARP configurations in a file called /etc/conf/local arp
- C. Add the proxy ARP configurations in a file called \$FWDIR/conf/local arp
- D. Add the proxy ARP configurations in a file called \$CPDIR/conf/local arp

**Answer: D**

#### NEW QUESTION 313

- (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 318

- (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 319**

- (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 323**

- (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 325**

- (Exam Topic 4)

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

**Answer:** B

**NEW QUESTION 328**

- (Exam Topic 4)

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

- A. cprod\_util MgmtlsPrimary
- B. cprod\_util FwlsSecondary
- C. cprod\_util MgmtlsSecondary
- D. cprod\_util FwlsPrimary

**Answer:** A

**NEW QUESTION 330**

- (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 333**

- (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 334**

- (Exam Topic 4)

When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

- A. Toni? AND 10.0.4.210 NOT 10.0.4.76
- B. To\*\* AND 10.0.4.210 NOT 10.0.4.76
- C. Ton\* AND 10.0.4.210 NOT 10.0.4.75
- D. "Toni" AND 10.0.4.210 NOT 10.0.4.76

**Answer:** D

#### NEW QUESTION 339

- (Exam Topic 4)

The Check Point history feature in R81 provides the following:

- A. View install changes and install specific version
- B. View install changes
- C. Policy Installation Date, view install changes and install specific version
- D. Policy Installation Date only

**Answer:** D

#### NEW QUESTION 343

- (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 344

- (Exam Topic 4)

What is Dynamic Balancing?

- A. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput
- B. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load
- C. It is a new feature that is capable of dynamically reserve the amount of Hash kernel memory to reflect the resource usage necessary for maximizing the session rate.
- D. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces

**Answer:** B

#### NEW QUESTION 345

- (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 346

- (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 347

- (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 349**

- (Exam Topic 4)

SmartEvent Security Checkups can be run from the following Logs and Monitor activity:

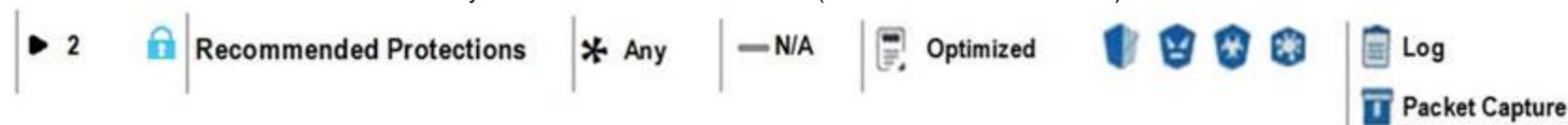
- A. Reports
- B. Advanced
- C. Checkups
- D. Views

**Answer:** A

**NEW QUESTION 352**

- (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 present
- 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\\_](https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_)

**NEW QUESTION 357**

- (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 358**

- (Exam Topic 4)

What component of Management is used for indexing?

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

**Answer:** D

**Explanation:**

[https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP\\_R80.30\\_Multi-DomainSecurityManag](https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Multi-DomainSecurityManag)

**NEW QUESTION 359**

- (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 to 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 362**

- (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 364**

- (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?

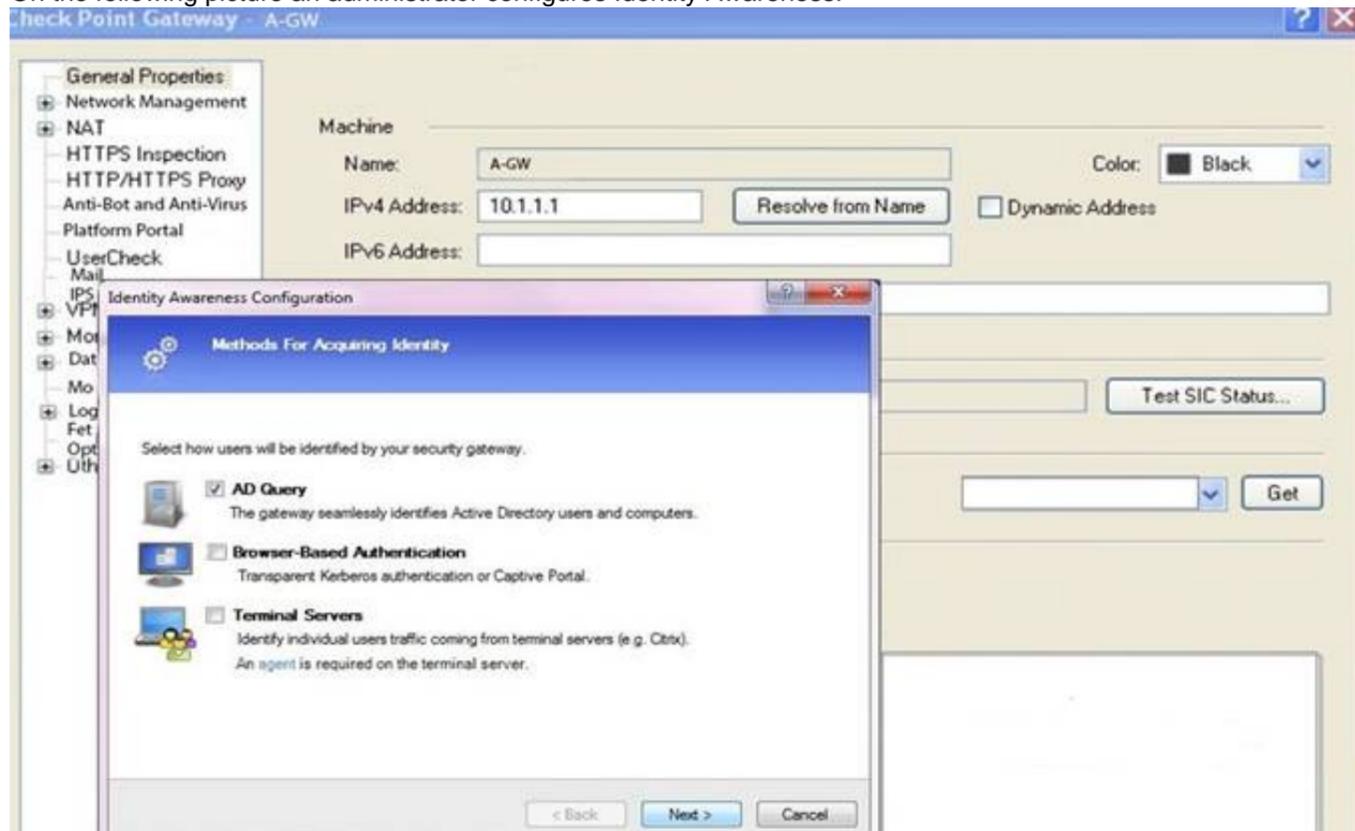
- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R81 gateways.

**Answer: A**

**NEW QUESTION 369**

- (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 371**

- (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 376**

- (Exam Topic 4)

What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

- A. test\_connectivity\_ad -d <domain>
- B. test\_ldap\_connectivity -d <domain>
- C. test\_ad\_connectivity -d <domain>
- D. ad\_connectivity\_test -d <domain>

**Answer: C**

**Explanation:**

[https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/CP\\_R81.30\\_CLI\\_ReferenceGuide/html\\_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/CP\\_R81.30\\_CLI\\_ReferenceGuide/200877](https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/200877)

**NEW QUESTION 377**

- (Exam Topic 4)

Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

- A. \$FWDIR/conf/client.scv
- B. \$CPDIR/conf/local.scv
- C. \$CPDIR/conf/client.svc
- D. \$FWDIR/conf/local.scv

**Answer:** D

**Explanation:**

[https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP\\_R81.10\\_RemoteAccessVPN\\_AdminG](https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG)

**NEW QUESTION 381**

- (Exam Topic 4)

Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

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

**Answer:** D

**NEW QUESTION 382**

- (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 387**

- (Exam Topic 4)

Which two Cluster Solutions are available under R81.10?

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

**Answer:** D

**NEW QUESTION 392**

- (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 394**

- (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](https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm)

#### NEW QUESTION 398

- (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 403

- (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 404

- (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 XMfifile and analysis of SOLR documents

**Answer: D**

#### NEW QUESTION 405

.....

## 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](#)